

# Sophos Mobile Control

## Technical guide

Product version: 2

Document date: December 2011



# Contents

- 1. About Sophos Mobile Control..... 3
- 2. Integration..... 4
- 3. Architecture..... 6
- 4. Workflow..... 12
- 5. Directory Access..... 15
- 6. Microsoft Exchange ActiveSync Proxy..... 16
- 7. Security ..... 17
- 8. Technical support ..... 18
- 9. Legal notices ..... 19

# 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 SMS messages. This manual describes the system's architecture and workflow.

Sophos Mobile Control currently supports the following mobile device platforms:

- Apple iOS
- Android
- 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.

## 1.1 Terms

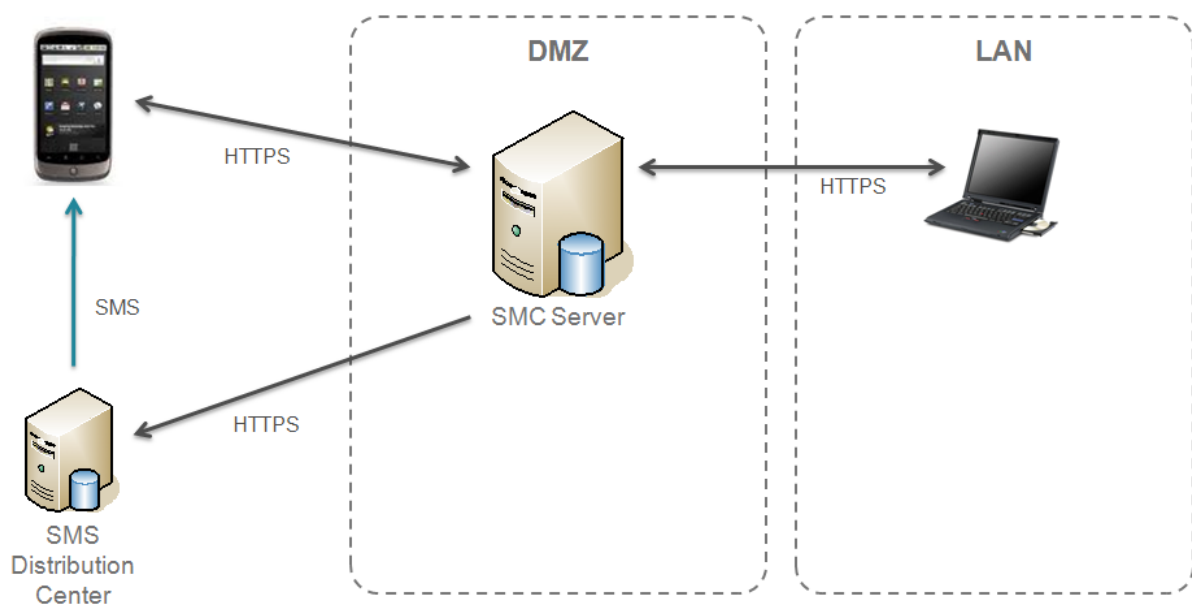
Term or Abbreviation	Description
APN	Access point name (to wireless network's data services)
DM	Device Management
DS	Data Synchronization
IMEI	Unique serial number of a mobile device
LDAP	Lightweight Directory Access Protocol
OMA	Open Mobile Alliance
OTA	over-the-air
SMS	Short Message Service
SSP	Self Service Portal
SyncML	Synchronization Markup Language
WAP	Wireless Application Protocol

## 2. Integration

The Sophos Mobile Control server (SMC server) can be integrated into the company's infrastructure as described in the following sections.

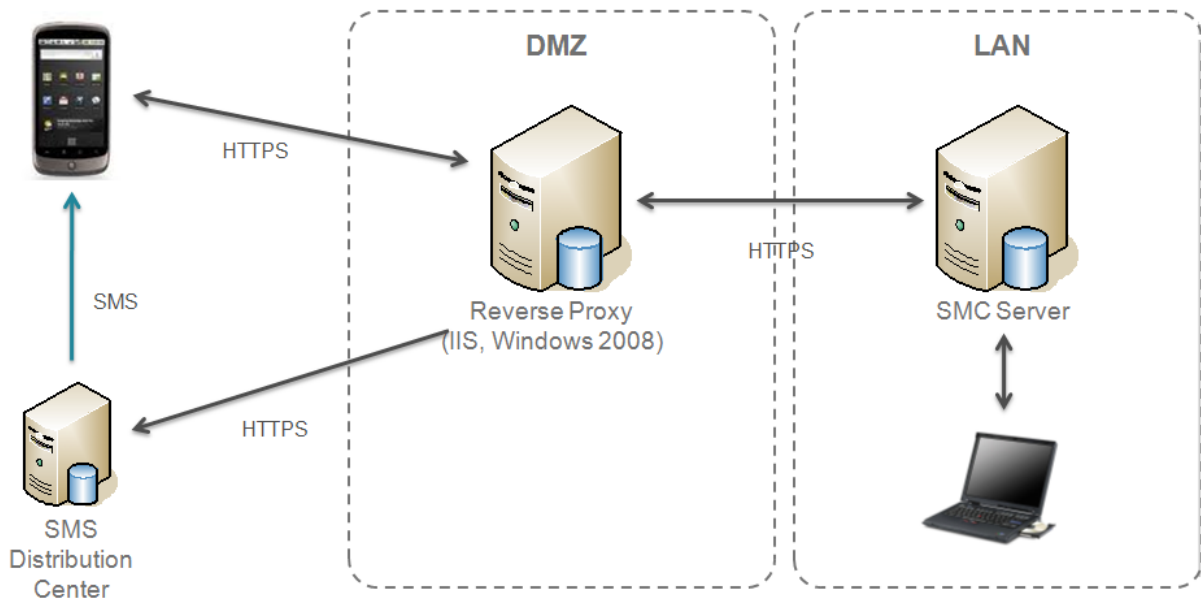
### 2.1 DMZ

SMC server can be installed in the DMZ network segment.



## 2.2 LAN

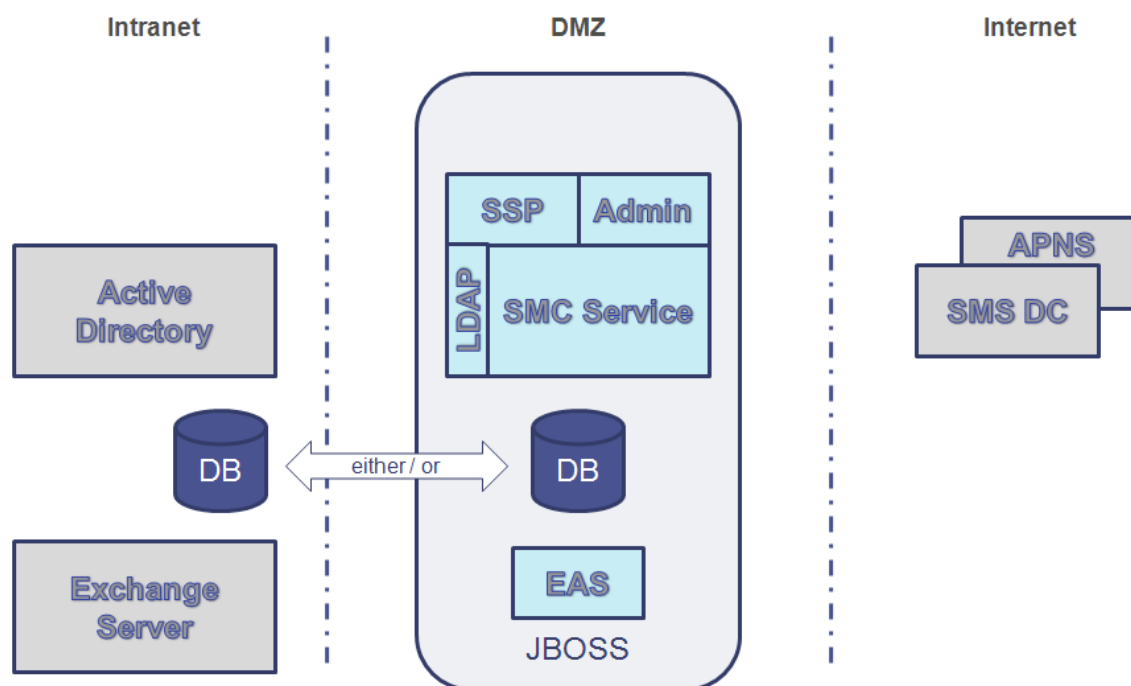
In this case, SMC server is installed in the LAN segment. A reverse proxy in the DMZ is used to allow incoming connections. The example shows an IIS server running on Windows 2008. This is our default option. Any other reverse proxy would also work.



## 3. Architecture

### 3.1 Overview

The following illustration shows both Sophos Mobile Control server and client and the network environment. Most of the mentioned components are described later in this manual.



### 3.2 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.
- The mobile devices synchronize with the server through HTTPS.
- The server relies on SMS to notify the clients. There are different options to set up SMS gateway connections.
- 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.

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.

### 3.2.1 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 SMS being sent or data being prepared for synchronization.

### 3.2.2 Web interface

#### 3.2.2.1 Administration web interface

The web interface is secured by a login and a session mechanism. The access control allows different user roles. The predefined roles are

- Administrator
- User
- Helpdesk

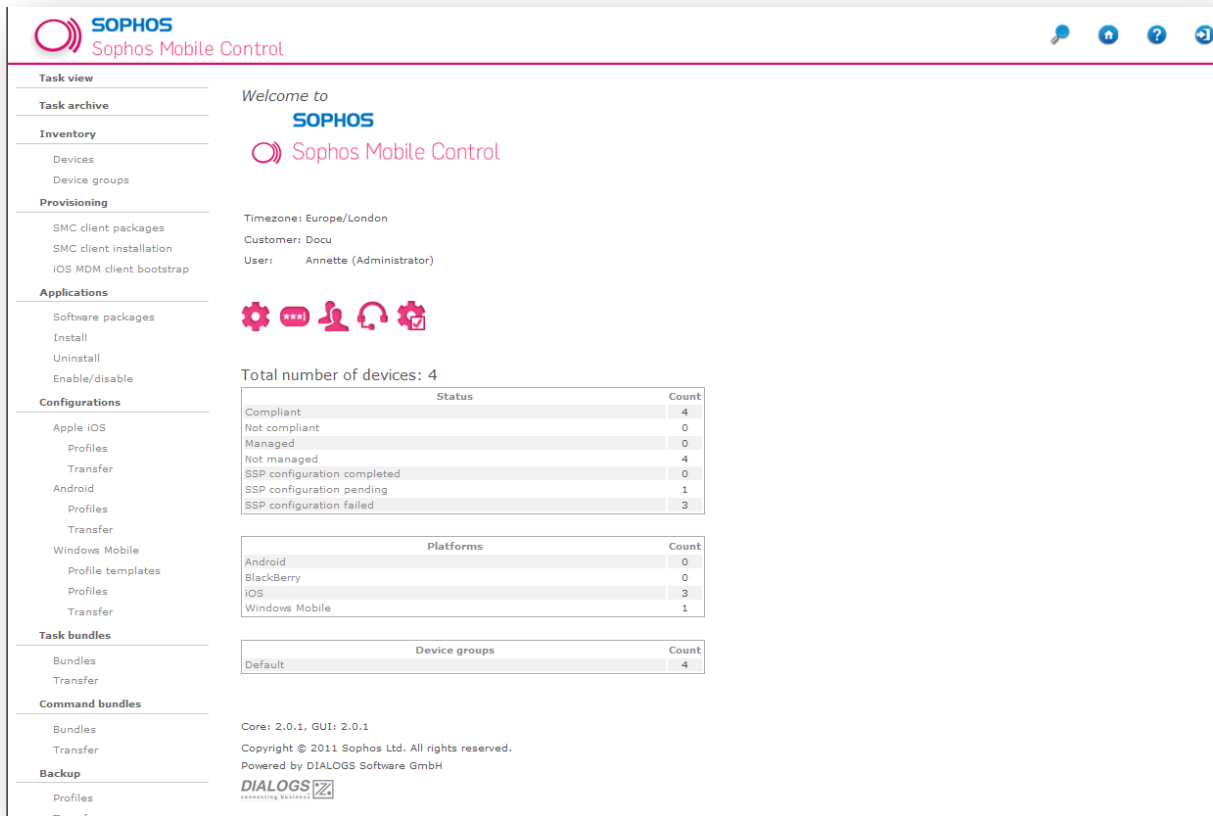
These roles have different sets of access rights. Users with the role Helpdesk for example, cannot delete software packages. The assignment of rights to roles can be set atomically. Additional roles can be created. Each user has exactly one role to define their access rights.

These are the most important modules of the web interface:

- Task view and archive
  - Used to monitor current and completed management operations including detailed status info.
- Inventory management
  - Used to keep track of registered devices and device groups.
- Provisioning
  - Used to provision new devices, that is installing the Sophos Mobile Control client or bootstrapping Apple MDM clients.
- Application management
  - Used to manage software packages and to (un-)install them on the devices.
- Configuration management
  - Used to set configurations and security policies on the devices (process white list, password policy, etc.).
- Command bundles
  - Used to define custom bundles of Sophos Mobile Control client commands to be transferred to the clients in a single task.

- User management
  - Used to manage the web interface users and roles.

Optional filters are available in many views of the web interface for restricting the number of items displayed. The creation of operations (software installations) is wrapped in wizards which are easy to use. All kinds of operations follow the same wizard structure which makes it easy to work with the web interface.



### 3.2.2.2 Self Service Portal

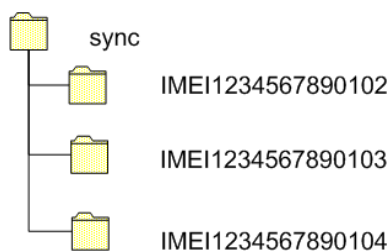
The Self Service Portal is secured by a login and a session mechanism. The account has to be set up by the administrator of the server and can be associated with any tenant. It is designed for the end users of devices and enables them to perform the provisioning process and MDM client bootstrap process of the device by themselves. The end users are also allowed to perform a remote lock or remote wipe. They can create any number of devices. Starting from the Sophos Mobile Control login view, end users can access the Self Service Portal by pointing the web browser to the Self Service Portal URL.

### 3.2.3 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.

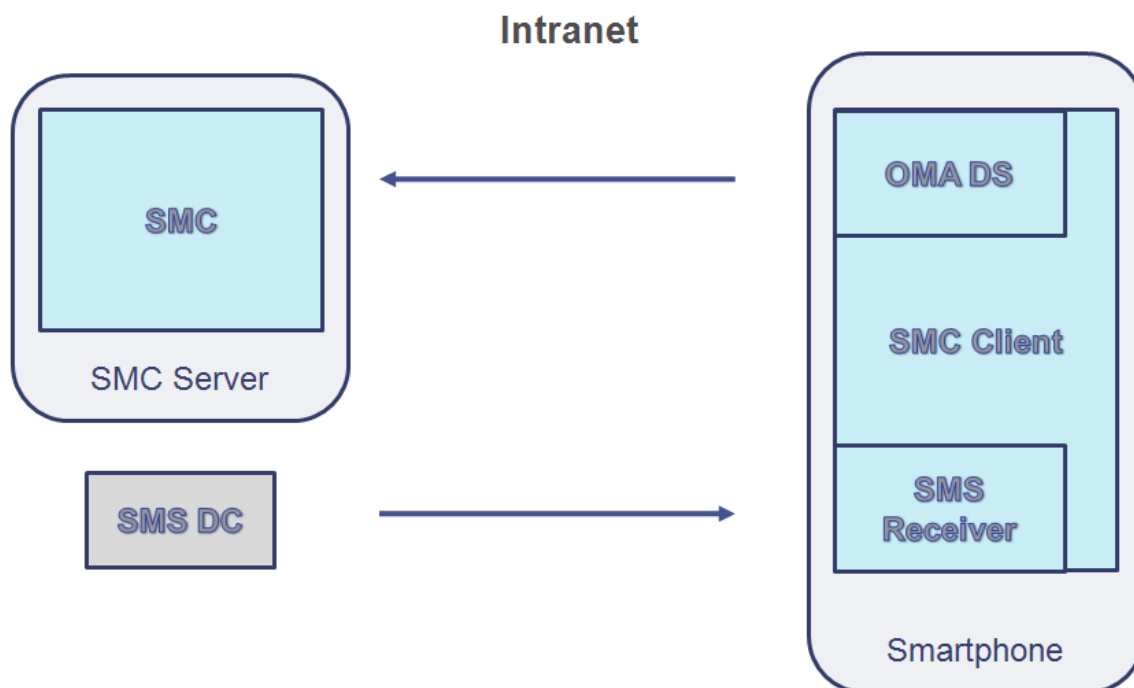
### 3.2.4 File system

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.



### 3.3 Client overview

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



#### 3.3.1 Apple iOS MDM-Client

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

#### 3.3.2 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 management commands from the server and handles them. It also monitors specific actions of the device and reports them to the server (for example software installations by the user). The following list explains the most important modules.

##### 3.3.2.1 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.

### **3.3.2.2 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.

### **3.3.2.3 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.

### **3.3.2.4 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.

### **3.3.2.5 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. Sophos Mobile Control does not need an “always online” mode. Connections are only opened when needed to enhance device standby time and reduce costs (depending on the device’s data plan).

#### **4.1.1 Trigger**

Synchronization is either triggered by a command of the administrator followed by an SMS message of the Sophos Mobile Control server, or as a result of a user-initiated action on the device.

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

- An application is being installed or uninstalled on the device.
- The traffic counter has reached a defined limit and causes enforced synchronization to communicate the current amount of transferred data to the server.
- The client has not contacted the server for a certain period of time.

The Sophos Mobile Control server sends SMS 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

#### **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 SMS inbox is monitored for an incoming SMS message containing a trigger word. (The SMS messages are retrieved before the device's messaging application notifies the user.)
2. After parsing the SMS 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.

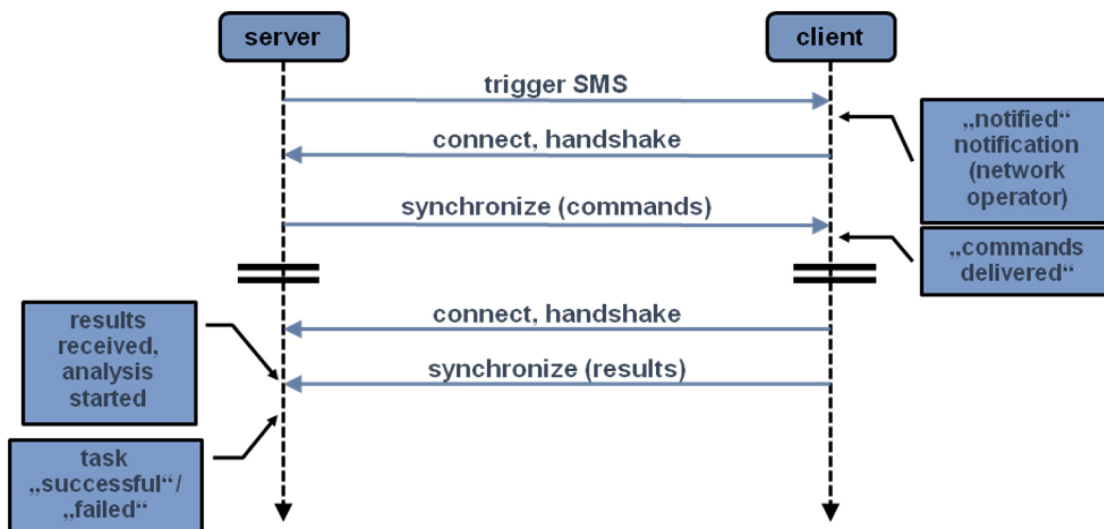
## 4.2 Installation and usage of the Sophos Mobile Control client

For installing a Sophos Mobile Control client on a mobile device, synchronization cannot be used, because the client is not yet installed. So 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. The user has to open the link and accept installation.



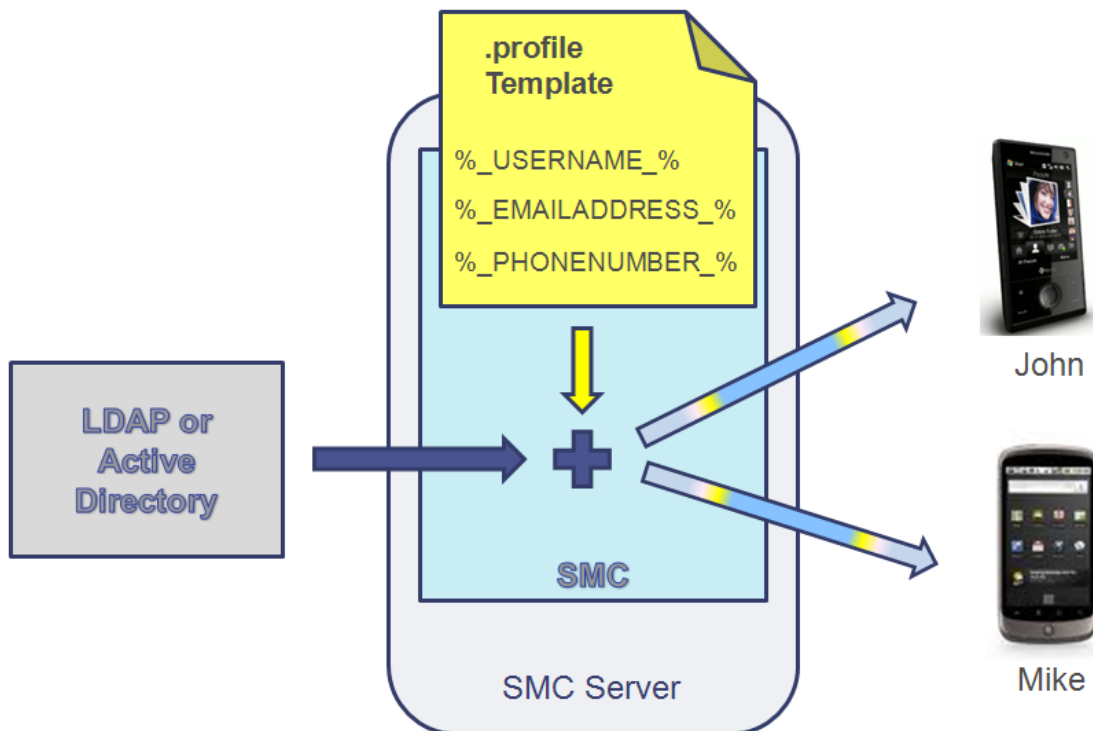
After client installation, specific information of the device is collected and sent to the server during the first synchronization process.

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



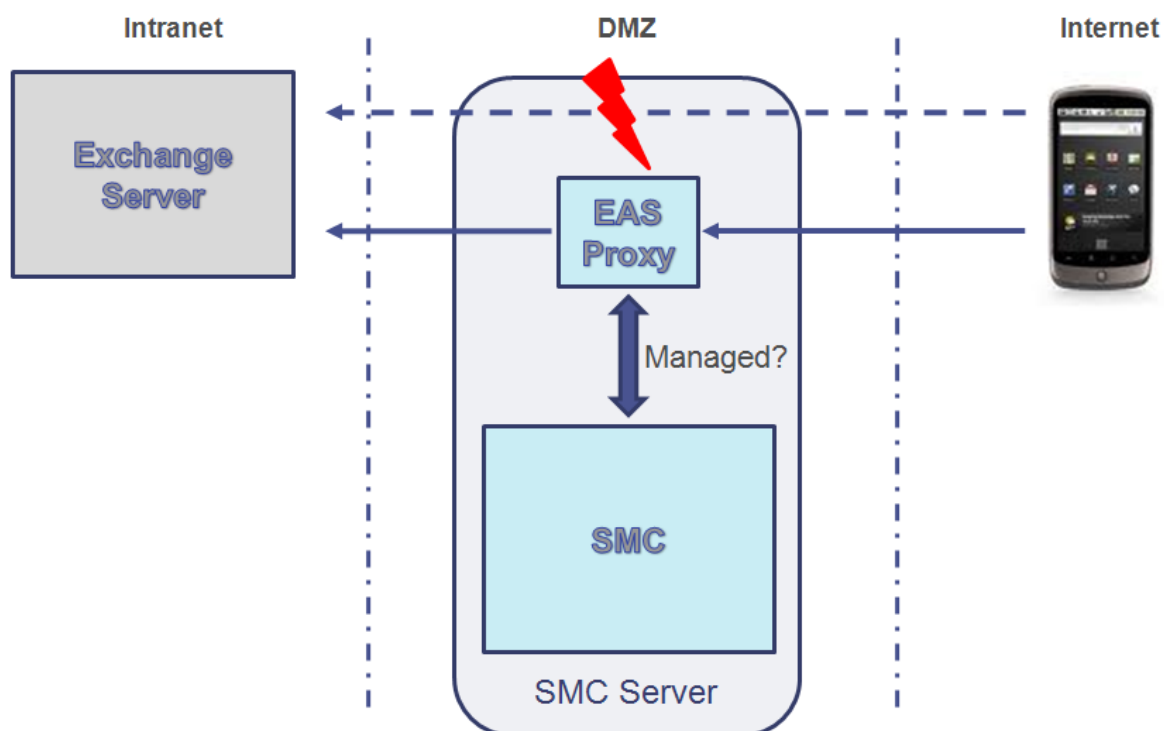
## 5. Directory Access

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. 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.



## 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. 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 via the web interface.



The EAS proxy component can be installed on the same server as Sophos Mobile Control. It can also be installed on any other machine that has access to the Sophos Mobile Control database and the Microsoft Exchange server.

## **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.

### **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 using a standard SSL/HTTPS connection and a server certificate.

The Sophos Mobile Control client authenticates itself 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. Technical support

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

- Visit the SophosTalk forum 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/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## **9. Legal notices**

Copyright © 2011 Sophos Ltd. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Powered by DIALOGS Software GmbH