SOPHOS
Security made simple.

Sophos Mobile Control
Installation prerequisites form

Product version: 6
Document date: December 2015

Contents

1 About this document 3

2 System environment 3

3 Communication between devices and push servers 12

4 Technical support 13

5 Legal notices 14

1 About this document

This document provides a check list for installation requirements for Sophos Mobile Control.
All required information has to be provided to ensure that the Sophos Mobile Control server runs properly on your network configuration.

Note: In this document, SMC is used as an abbreviation for Sophos Mobile Control.

2 System environment

2.1 Mobile devices

Please specify which device type(s) you plan to use with Sophos Mobile Control.

☐ Apple iPhone with iOS 7 (or higher, Apple ID required)

☐ Apple iPad or iPod Touch with iOS 7 (or higher, Apple ID required)

☐ Android 4.0 (or higher)

☐ Windows Phone 8

☐ Windows Phone 8.1

☐ Windows 10 Mobile

2.2 Server SSL Certificate

Please specify if you want to use an officially signed or a self-signed certificate for the Sophos Mobile Control web interface.

Android software packages like the SMC MDM client can only be downloaded from https servers with an officially signed certificate.

Use self-signed certificate	☐ (Android software installation not possible)
Use existing official certificate signed by, for example, VeriSign or GoDaddy	☐ (Android software installation possible)

Note: The certificate should be provided in a PKCS#12 file including all certificates in the certificate path.

Note: For self-signed certificates and Windows Phone 8 or higher devices, the SSL certificate needs to be installed on the devices before devices can be managed.

2.3 Operating system for SMC server

Please specify which server operation system you want to use.

☐ Windows Server 2008 (64 bit)

☐ Windows Server 2008 R2 (64 bit)

☐ Windows Server 2012 (64 bit)

☐ Windows Server 2012 R2 (64 bit)

2.4 Other

Please make sure that the following applies:

No IIS installed and no other application using ports 80, 443.	☐

2.5 Database

Please specify which database management system you want to use.

Shipped with SMC installer

☐ Microsoft SQL Server 2014 Express (64 bit)

or

Existing database

☐ Microsoft SQL Server 2008 (32 bit, 64 bit)

☐ Microsoft SQL Server 2008 R2 (64 bit)

☐ Microsoft SQL Server 2012 (64 bit)

☐ Microsoft SQL Server 2014 (64 bit)

☐ Microsoft SQL Server 2014 Express (64 bit)

☐ MySQL 5.6

Microsoft SQL Server must have Windows authentication or SQL server authentication.

If you use Microsoft SQL Server Express, please make sure that the management tools are also installed.

Use existing database server	☐
Existing SQL account with sysadmin role (no AD credentials)	
Have access to SQL management tools (separate install for Express)	☐
TCP IP enabled	☐
SQL browser service is enabled (Useful only, if an external database is used.)	☐
Language for used SQL login is English	☐

2.6 LDAP configuration

If SMC is to be used with the Self Service Portal enabled, create an LDAP group containing all users who should get access to the Self Service Portal. You can use * to grant access to all authenticated users.

LDAP group name	

2.7 Network details

Please provide the information required for pre-configuring your Sophos Mobile Control server installation.

External IP address of the SMC server	
Internal IP address of the SMC server (if different from external)	
DNS name of the SMC server (for example mobilecontrol.corporate.com) Please make sure that this can be resolved over the internet.	
IP address or hostname and port of the database server (for example 127.0.0.1:1433 for MS SQL Server or 127.0.0.1:3306 for MySQL)	
Use SSL to connect to MS SQL Server	☐
IP address or hostname of the corporate SMTP server	
User name and password for authentication with SMTP are known (if required).	
Optional EAS Proxy: URL of Exchange ActiveSync Server (for example *exchange.corporate.com*) **Note:** If your current exchange denies IOS, Windows Phone or Android devices, this will need to be modified for EAS to work.)	
Use SSL to connect to Exchange ActiveSync server	☐
Optional LDAP support: Corporate LDAP Server for personalized profiles (for example ldap.corporate.com:389)	
Use SSL to connect to LDAP server (for example ldap.coporate.com:636)	☐
User name and password for authentication with LDAP are known.	☐

Optional SCEP support: URL of Certification Authority with SCEP support for iPhones (for example http://ca.corporate.com/certsrv/mscep/mscep.dll)	

2.8 Firewall

The following ports of the Sophos Mobile Control server have to be reachable from the internet.

2.8.1 Allow traffic from corporate LAN and the internet

Port	Protocol	Description	Setup successful
80	HTTP	Forwards to HTTPS-Port	☐
443	HTTPS	Access to web interface / synchronization data (in\out bound)	☐

2.8.2 Allow traffic from SMC server to database host

Note: If no local database installation is used.

Port	Protocol	Description	Setup successful
1433	MS SQL Server	Database access	☐
3306	MySQL Server	Database access	☐

2.8.3 Allow traffic from SMC server to SMTP host

Port	Protocol	Description	Setup successful
25 465 587	SMTP or SMPTS or SMTP/TLS	Send error reports by e-mail, roll-out of devices, distribution of passwords and notification of administrators in case of compliance violations and notification by email on expiry of APNS certificates.	☐

2.8.4 Allow traffic from SMC server to Sophos Service Center

The Sophos Service Center is used for iOS, Windows Phone push messages (MPNS) and Baidu Push for the SMC apps, for example for compliance violation notifications.

Knowledge Base Article #120875 explains in which cases which data is sent via Sophos servers.

Port	Protocol	Description	Setup successful
443	TCP	SSL secured connection to IP address 85.22.154.49 (services.sophosmc.com)	☐

2.8.5 Optional: Allow traffic from SMC server to Exchange and LDAP

Port	Protocol	Description	Setup successful
80 or 443	HTTP/S	CA server with SCEP	☐
389 or 636	LDAP/S	LDAP connection (plain or SSL-protected)	☐

2.8.6 Optional: Allow traffic from SMC server to SCEP server

Port	Protocol	Description	Setup successful
80 or 443	HTTP/S	CA server with SCEP	☐

2.8.7 Optional: Allow traffic from SMC server to Apple Volume Purchasing Program (VPP)

Port	Protocol	Description	Setup successful
443	HTTPS	Apple VPP server IP address: 17.0.0.0/8	☐

2.8.8 For iOS devices: Allow traffic from SMC server to APNS

iOS devices receive notifications over the Apple Push Notification service (APNS).
You need to create your own APNs certificate to use with Sophos Mobile Control for the connection to Apple:

http://www.apple.com/iphone/business/integration/mdm/

Port	Protocol	Description	Setup successful
2195	TCP/SSL	gateway.push.apple.com (IP addresses: 17.*.*.*)	☐

2.8.9 For iOS devices: Allow traffic from SMC server to Apple iTunes service

Port	Protocol	Description	Setup successful
443	HTTPS	itunes.apple.com (IP addresses: 17.*.*.*)	☐

2.8.10 Optional: Allow traffic from SMC server to Apple Activation Lock Bypass service for supervised devices

Port	Protocol	Description	Setup successful
443	HTTPS	deviceservices-external.apple.com (IP addresses: 17.*.*.*)	☐

2.8.11 For Android devices: Allow traffic from SMC server to GCM

To trigger Android devices silently, Google offers Google Cloud Messaging (GCM).

Port	Protocol	Description	Setup successful

443	HTTPS	android.googleapis.com/ gcm-http.googleapis.com	☐

2.8.12 For Windows Phone devices: Allow traffic from SMC server to WNS

To trigger Windows Phone 8.1 devices silently, Microsoft offers the Windows Push Notification Service (WNS).

Port	Protocol	Description	Setup successful
443	HTTPS	login.live.com and db3.notify.windows.com	☐

2.9 Prerequisites for external EAS Proxy

Sophos Mobile Control offers a separate installer for configuring an external EAS Proxy (for example for load balancing). For the external EAS Proxy, several aspects have to be considered. Depending on usage scenario, the EAS Proxy cannot be addressed directly. With several customers (tenants) for example, a Reverse Proxy has to be used that directs the incoming traffic for each customer to a separate port (for example 8080, 8081 and so on). The EAS redirects the ActiveSync traffic to the configured Exchange Server.

Before you configure an external EAS Proxy, fill out the following checklist:

Which ports should the EAS Proxy use?	
Is a Reverse Proxy or something similar already available?	
Has redirection to the relevant ports been configured at the Reverse Proxy?	
External/internal IP/DNS name of the Reverse Proxy	
Where is the EAS Proxy to be installed (same machine as the SMC server or separate maschine)?	
IP address for the EAS Proxy (if installed on a separate machine)	
IP or DNS names of the Exchange Servers	
Is ActiveSync activated at the Exchange Server?	☐
Open Firewall from Reverse Proxy to EAS Proxy?	☐
Open Firewall from EAS Proxy to https port on SMC host?	☐
Open Firewall from EAS Proxy to http or https port on Exchange Servers?	☐

3 Communication between devices and push servers

3.1.1 For iOS devices: Allow traffic from device to Apple push server

For communication between iOS devices and the Apple Push server within a corporate WLAN, Port 5223 has to be open.

3.1.2 For Android devices: Allow traffic from device to Google Cloud Messaging Server

For communication between the Android device and the Google Cloud Messaging Server, connectivity with GCM has to be allowed. The following ports need to be open: 5228, 5229 and 5230. GCM typically only uses 5228, but sometimes 5229 and 5230 are used. GCM does not provide specific IPs, but changes them frequently.

4 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* including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

5 Legal notices