SOPHOS
Security made simple.

Sophos Mobile installation prerequisites form

Product version: 8.0

Contents

1 About this document

This document provides a checklist for the installation requirements of Sophos Mobile.

You must provide all required information to ensure that the Sophos Mobile server runs properly on your network configuration.

2 System environment

2.1 Managed devices

Specify which device types you want to use with Sophos Mobile. Check all that apply.

☐ **Apple iPhone with iOS 9.0 or higher**

☐ **Apple iPad or iPod Touch with iOS 9.0 or higher**

☐ **Apple Mac with macOS 10.11 or higher**

☐ **Android 4.4 or higher**

☐ **Windows Phone 8.1**

☐ **Windows 10 Mobile or Mobile Enterprise**

☐ **Windows 10 Pro, Enterprise, Education, Home or S**

2.2 Server SSL Certificate

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

○ **Self-signed certificate (Android app package installation not possible)**

○ **Existing official certificate signed by, for example, VeriSign or GoDaddy**

If you want to use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), you must manually install that self-signed certificate or your CA certificate on your devices before enrolling them with Sophos Mobile.

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

2.3 Operating system for the Sophos Mobile server

Specify which server operation system you want to use:

- ○ **Windows Server 2008 R2 SP1 (64-bit)**
- ○ **Windows Server 2012 (64-bit)**
- ○ **Windows Server 2012 R2 (64-bit)**
- ○ **Windows Server 2016 (64-bit)**

2.4 Other

Make sure that the following applies:

☐ **No IIS installed and no other application using ports 80 or 443**

2.5 Database

Specify which database server you want to use:

- ○ **new Microsoft SQL Server 2014/2016 Express (64 bit), created by Sophos Mobile installer**
- ○ **existing Microsoft SQL Server 2008 SP4 (32 bit or 64 bit)**
- ○ **existing Microsoft SQL Server 2008 R2 SP3 (64 bit)**
- ○ **existing Microsoft SQL Server 2012 (64 bit)**
- ○ **existing Microsoft SQL Server 2014 (64 bit)**
- ○ **existing Microsoft SQL Server 2014 Express (64 bit)**
- ○ **existing Microsoft SQL Server 2016 (64 bit)**
- ○ **existing Microsoft SQL Server 2016 Express (64 bit)**
- ○ **existing MySQL 5.6**

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

Existing SQL account with sysadmin role (no AD credentials)

☐ **SQL management tools have been installed (required for Microsoft SQL Server Express)**

☐ **TCP IP is enabled**

☐ **The SQL browser service is enabled (useful only if an external database is used)**

☐ **The language of the account that is used to log in to SQL is set to English**

2.6 LDAP configuration

If you want to use the Sophos Mobile Self Service Portal, create an LDAP group containing all users who need to access the Self Service Portal. Alternatively, you can use * to grant access to users of all LDP groups.

LDAP group name

2.7 Network details

Provide the required information for pre-configuring your Sophos Mobile server installation.

External IP address of the Sophos Mobile server

Internal IP address of the Sophos Mobile server (if different from external)

DNS name of the Sophos Mobile server.
Example: *mobilecontrol.yourcompany.com*

Note: Make sure that the DNS name can be resolved over the internet.

IP address or hostname and port of the database server.
Example: *127.0.0.1:1433* (for MS SQL Server), *127.0.0.1:3306* (for MySQL)

IP address or hostname of your corporate SMTP server

☐ **SSL/TLS is used to connect to the MS SQL Server**

☐ **User name and password for SMTP authentication are known (if required)**

For the optional EAS proxy, the URL of the Exchange ActiveSync server
Example: *exchange.yourcompany.com*

Note: For EAS to work, you also must configure your Exchange server to allow access by iOS, Windows Phone/Mobile and Android devices.

☐ **SSL/TLS is used to connect to the Exchange ActiveSync server**

For optional LDAP support, your corporate LDAP server for personalized profiles
Example: *ldap.yourcompany.com:389*

☐ **SSL/TLS is used for connects to the LDAP server. Example: *ldap.yourcompany.com:636***

☐ **User name and password for LDAP authentication are known**

For optional SCEP support, the URL of Certification Authority with SCEP support for iPhones
Example: *http://ca.yourcompany.com/certsrv/mscep/mscep.dll*

2.8 Firewall

The following ports of the Sophos Mobile server must be reachable from the internet.

2.8.1 Allow traffic from corporate LAN and the internet

Port	Protocol	Description	Available?
80	HTTP	Forwards to HTTPS-Port	☐
443	HTTPS	Access to web interface and for data synchronization (inbound/outbound)	☐

2.8.2 Allow traffic from Sophos Mobile server to database host

Note: If no local database installation is used.

Port	Protocol	Description	Available?
1433	MS SQL server	Database access	☐
3306	MySQL server	Database access	☐

2.8.3 Allow traffic from Sophos Mobile server to SMTP host

Port	Protocol	Description	Available?
25 465 587	SMTP or SMPTS or SMTP/TLS	Send error reports by email for device enrollment, distribution of passwords, and notification of administrators in case of compliance violations or expiry of APNs certificates.	☐

2.8.4 Allow traffic from Sophos Mobile server to Sophos Service Center

The Sophos Service Center is used for iOS, Windows Phone push messages (MPNS, WNS) and Baidu Push for the Sophos Mobile 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	Available?
443	TCP	SSL secured connection to IP address 85.22.154.49 (services.sophosmc.com)	☐

2.8.5 Allow traffic from Sophos Mobile server to Google reCAPTCHA

The Google reCAPTCHA service is used by the Sophos Mobile login pages.

Port	Protocol	Description	Available?
443	TCP	www.google.com/recaptcha	☐

2.8.6 Optional: Allow traffic from Sophos Mobile server to Exchange and LDAP

Port	Protocol	Description	Available?
80 or 443	HTTP/S	Exchange server for EAS proxy	☐
389 or 636	LDAP/S	LDAP connection (plain or SSL-protected)	☐

2.8.7 Optional: Allow traffic from Sophos Mobile server to SCEP server

Port	Protocol	Description	Available?
80 or 443	HTTP/S	CA server with SCEP	☐

2.8.8 Optional: Allow traffic from Sophos Mobile server to SGN server

Sophos Mobile can synchronize corporate keyrings from Sophos Safeguard Enterprise (SGN) to the Sophos Secure Workspace app.

Port	Protocol	Description	Available?
80 or 443	HTTP/S	Your SGN server	☐

2.8.9 For iOS and macOS devices: Allow traffic from Sophos Mobile server to APNs

iOS and macOS devices receive notifications over the Apple Push Notification service (APNs).

You need to create your own APNs certificate to use with Sophos Mobile for the connection to Apple.

Port	Protocol	Description	Available?
2195	TCP/SSL	gateway.push.apple.com (IP address: 17.0.0.0/8)	☐

2.8.10 For iOS and macOS devices: Allow traffic from Sophos Mobile server to Apple iTunes service

Port	Protocol	Description	Available?
443	HTTPS	itunes.apple.com (IP address: 17.0.0.0/8)	☐

2.8.11 For iOS devices (optional): Allow traffic from Sophos Mobile server to Apple Volume Purchasing Program (VPP)

Port	Protocol	Description	Available?
443	HTTPS	vpp.itunes.apple.com IP address: 17.0.0.0/8	☐

2.8.12 For iOS devices (optional): Allow traffic from Sophos Mobile server to Apple Device Enrollment Program (DEP)

Port	Protocol	Description	Available?
443	HTTPS	mdmenrollment.apple.com IP address: 17.0.0.0/8	☐

2.8.13 For iOS devices (optional): Allow traffic from Sophos Mobile server to Apple Activation Lock Bypass service for supervised devices

Port	Protocol	Description	Available?
443	HTTPS	deviceservices-external.apple.com (IP address: 17.0.0.0/8)	☐

2.8.14 For Android devices: Allow traffic from Sophos Mobile server to GCM

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

Port	Protocol	Description	Available?
443	HTTPS	android.googleapis.com gcm-http.googleapis.com	☐

2.8.15 For Android devices: Allow traffic from Sophos Mobile server to Google service for Android enterprise

To manage a work profile on Android devices (Android enterprise), Sophos Mobile must communicate with Google API services.

Port	Protocol	Description	Available?
443	HTTPS	www.googleapis.com	☐

2.8.16 For Windows devices: Allow traffic from Sophos Mobile server to Windows push notification servers

To trigger Windows and Windows Mobile devices silently, Microsoft offers push notification services.

Port	Protocol	Description	Available?
443	HTTPS	login.live.com *.notify.windows.com	☐

2.9 Prerequisites for standalone EAS proxy

Sophos Mobile offers a separate installer for configuring a standalone 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?

What is the external/internal IP/DNS name of the Reverse Proxy?

Will the EAS proxy be installed on the same computer as the Sophos Mobile server or on a separate computer?

If installed on a separate computer, what is the IP address for the EAS proxy?

What are the IP or DNS names of the Exchange servers?

☐ **ActiveSync is activated on the Exchange servers**

☐ **Firewall allows communication between the Reverse Proxy and the EAS proxy**

☐ **Firewall allows communication between the EAS proxy and the https port on the Sophos Mobile host**

☐ **Firewall allows communication between the EAS proxy and the http or https port on the Exchange servers**

3 Communication between devices and external servers

3.1.1 For iOS and macOS devices: Allow communication with APNs

Port	Destination	Description	Available?
5223	17.0.0.0/8	Communication between iOS and macOS devices and the Apple Push Notification service (APNs) within your corporate WLAN	☐

3.1.2 For iOS and macOS devices (optional): Allow communication with Apple update server

Port	Description	Available?
443	mesu.apple.com If not available, Sophos Mobile has no information about iOS and macOS updates. For example, compliance rules regarding mandatory updates have no effect.	☐

3.1.3 For Android devices: Allow communication with GCM

Port	Description	Available?
5228, 5229, 5230	Communication between Android devices and the Google Cloud Messaging (GCM) service. Typically, GCM only uses port 5228, but ports 5229 and 5230 are used occasionally as well. IP addresses for GCM are changed frequently.	☐

3.1.4 For Windows devices: Allow communication with Windows push notification services (MPNS, WNS)

Port	Destination	Available?
442	*.notify.live.net, *.wns.windows.com, *.notify.windows.com	☐

4 Technical support

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

- Visit the Sophos 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/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