1 About this guide

This guide contains deployment considerations for a Sophos Mobile system. It provides guidance on the proper dimensioning of a Sophos Mobile server installation in terms of hardware (for example CPU and memory) and software (for example database and virtualization) requirements, and it explains, on the basis of schematic diagrams, different usage scenarios for the integration of Sophos Mobile and the standalone EAS proxy into your organization's infrastructure.
2 Sizing considerations

Important
This section provides guidance on how to size the Sophos Mobile server based on some key criteria. The recommendations are based on default settings of the relevant configuration parameters and on a reasonable distribution of device types, tenants (customers) and administrators. If the setup for a customer differs significantly, the suggested values must to be modified.

Activities that generate load

The following activities generate load on the Sophos Mobile server:

- **Administrator interaction**: Any administrator interactively working in a customer account generates load. The load depends on the amount of interactive actions and the number of devices for that customer.

- **Self Service Portal interaction**: Any user interactively working on the Self Service Portal generates load. The number of concurrent sessions is relevant for the sizing of a server.

- **Device Sync**: The devices synchronize with the server in predefined intervals. Each sync operation generates load. The number of devices and the interval are relevant for the sizing of a server.

- **Policy/app distribution**: Any device interaction, like lock or wipe, policy updates or app distribution generates server load. The server is able to distribute the load over time (batching), but the server must be sized to handle that additional load.

- **Email traffic**: The EAS proxy acts as a gateway for email communication. The server load depends on the number of devices syncing email and the sync period. If the EAS proxy is installed on a different server, this load can be neglected. More than one active EAS proxy can add to the server load, as the device status must be fetched regularly. Please note that, because all email traffic passes the EAS proxy, sufficient network bandwidth is required.

System components

A Sophos Mobile system can be divided into 3 main components:

- **Sophos Mobile server**: The server manages all administrator and user interactions, the device sync and the policy and app distribution.

- **Database server**: The database server (DB server) handles all read and write activities and queries. Most of the SMC server activities result in a DB server action. The DB server can be installed either on the same or different hardware server as the Sophos Mobile server.

- **EAS proxy**: All email traffic passes the EAS proxy. It is installed either as a component of the Sophos Mobile server (internal EAS proxy) or as a separate component on one or more external servers (standalone EAS proxy).

Sophos Mobile server sizing

Definitions:

- 1 CPU equals to an Intel XEON core with 2.5 GHz.
• Memory values are in GB.
• The SMC database is the only database on that SQL server.
• Sophos Mobile 9 latest patch level.
• Device default sync cycle of 24 hours.

<table>
<thead>
<tr>
<th># of devices</th>
<th>Sophos Mobile server</th>
<th>DB server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CPU</td>
<td>Memory</td>
</tr>
<tr>
<td>Up to 200</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Up to 500</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Up to 1.000</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Up to 2.000</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Up to 5.000</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Up to 10.000</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Up to 20.000</td>
<td>8</td>
<td>16</td>
</tr>
</tbody>
</table>

Sophos Mobile fully supports VMWare virtual environments. The sizing recommendations are expected to suit virtual environments as well. Because there might be some other influences on the virtualized servers, Sophos cannot confirm 100% matching performance in virtual environments.

Sophos Mobile has no hard limit at 20.000 devices. But any sizing beyond this requires detailed input on the parameter, like sync cycle, number of tenants, device mix and number of interactive users. Also, any sizing beyond 20.000 devices requires a cluster setup.

If you need to manage more than 20.000 devices, please contact product management.

**EAS proxy sizing**

Sophos Mobile offers two EAS proxy components. The internal EAS proxy is part of the Sophos Mobile server and can be used for a simple setup in smaller installations. The internal EAS proxy is recommended for installations with no more than 500 devices syncing emails and if no failover or clustering is required.

The standalone or external EAS proxy is recommended for larger installations, if device management and email proxy have to separate or clustering is required. The standalone EAS proxy does not require a lot of CPU and memory, the key limitation is bandwidth. Because the EAS proxy is critical for the delivery of email, the recommended setup for larger installations is to have multiple instances of EAS proxies with a load balancer before them.

Sizing recommendation for EAS proxy: 1 CPU and 2 GB of memory.
Database sizing

The size of the database depends on the following factors:

- The mobile platforms you want to manage (Android, iOS, macOS, Windows, Windows Mobile).
- The used database (MS-SQL or MySQL).
- The data on the mobile devices (e.g. the number of installed apps).
- Apps to be published on the Sophos Mobile server.
- Documents to be published on the Sophos Mobile server.

Some real world examples show 0.2 MB per device, thus a 500 device server uses 25 MB.

On most customer installation, the required database size is strongly influenced by the number of apps and documents published through Sophos Mobile.

For installation beyond 500 devices, you should consider using an MS-SQL Standard server instead of an MS SQL Express edition.

Network sizing

To properly size the network connection to Sophos Mobile, please use the following data as a guideline. An Sophos Mobile managed device normally synchronizes once a day with the server. In this synchronization cycle, information like device properties, security information, app list and certificates are exchanged. On an average device, please calculate the following data usage per device:

<table>
<thead>
<tr>
<th>Device type</th>
<th>Data volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>50 KB</td>
</tr>
<tr>
<td>iPhone, iPad</td>
<td>100 KB</td>
</tr>
<tr>
<td>Mac</td>
<td>150 KB</td>
</tr>
<tr>
<td>Windows Mobile/Phone</td>
<td>100 KB</td>
</tr>
<tr>
<td>Windows computer</td>
<td>100 KB</td>
</tr>
</tbody>
</table>

The majority of network traffic is generated by the distribution of apps, documents and policies to the devices. The network sizing should take this into account. The server handles any of these device interactions in batches of 500 devices to avoid overloading of the server and the network. Apps and documents can be calculated with an overhead of 10% of the app or document size. A policy push is about the same size as a device sync.

Sophos Mobile Security data usage

Sophos Mobile Security is a security app for Android devices that protects devices from malicious apps and assists end users in detecting app permissions that could be a security risk. Its web filtering capability allows you to filter websites by category and lets you block inappropriate content.

On devices that have the Sophos Mobile Security app installed, the following network traffic occurs:
- On each malware scan, 256 bytes per app are used for online look-ups against the latest threat data in the SophosLabs database.
- For downloading data updates for the antivirus engine, 10-20 KB per day are used on average.
3 Architecture examples

Learn how to integrate Sophos Mobile server into your organization’s infrastructure.

Communication overview
Sophos Mobile in DMZ with incoming and outgoing traffic protection

DMZ
- Sophos UTM, Cisco ISE, Check Point, NAC
- SMAC Server or Cluster
- Proxy

LAN
- Admin GUI & SSP
- Web service API
- MS SQL/MySQL (local or remote)
- SMTP (plain, SSL or TLS)
- LDAP
- Exchange Server or Traveler Server
- S3N Server

Required
Optional

Apple Volume Purchase Program
vpp.intras-apple.com
Apple App identifier search
itunew.apple.com
Apple Activation Lock Bypass
device.services.external.apple.com
Apple Device Enrollment Program
mdm.apple.com厭
Intune app protection, Federated Auth with Azure
login.microsoftonline.com, graph.microsoft.com
TeamViewer
login.teamviewer.com, webapi.teamviewer.com, start.teamviewer.com

Google FCM
android.googleapis.com, fcm.googleapis.com
Android Enterprise
www.googleapis.com
ReCaptcha
www.google.com/recaptcha/apk/hiliterify
Microsoft WINS
login.live.com, *-notify.windows.com
Apple Push Notification service
aps.push.apple.com (127.0.0.1 or 443)
Sophos service center
services.sophos.com
Sophos Mobile in backend with incoming and outgoing traffic protection

- Apple Volume Purchase Program
- Apple App Identifier search
- iTunes.apple.com
- Apple Activation Lock Bypass
deviceservices-external.apple.com
- Apple Device Enrollment Program
- mdm enrollment.apple.com
- Intune app protection, Federated Auth with Azure
- login.microsoftonline.com, graph.microsoft.com
- Teamsviewer
- login.teamviewer.com, webapp.teamviewer.com, start.teamviewer.com
- Google TCM
- android.googleapis.com, fcm.googleapis.com
- Android Enterprise
- www.googleapis.com
- ReCaptcha
- www.google.com/recaptcha/api/verify
- Microsoft MDM
- login.live.com, "microsoft.windows.com
- Apple Push Notification service
- api.push.apple.com (170.170.170.1:443)
- Sophos service center
- ‏services.sophosmc.com

DMZ
Sophos UTM, Cisco ISE, Check Point, NAC

LAN
Admin GUI & SSP
Webservice API

SMC Server or Cluster
tcp 3006 or tcp:1433

MS SQL/MySQL
(local or remote)

WAF
https

Proxy
https

Lan
https

SMTP Server
smtp (plain, SSL or TLS)

LDAP Server
ldap/s

Exchange Server or Traveler Server
http/s

SGN Server
http/s
Sophos Mobile as a Service communication overview

- Customer network:
  - Exchange Server or Traveler Server
  - EAS Proxy
  - Sophos UTM, CiscoISE, Check Point, NAC
  - Admin GUI & SSP
  - User directory

- Sophos data center:
  - SMC
  - Database
  - SMTP

- Push services, Apple VPP, Apple App Identifier search, Activation Lock Bypass, Device Enrollment Program, Android Enterprise, Intune, Intune app protection

Copyright © Sophos Limited
Sophos Mobile cluster with Sophos UTM Web Application Firewall

- Push services, Apple VPP, Apple App Identifier search, Activation Lock Bypass, Device Enrollment Program, Android Enterprise, ReCaptcha, Intune app protection

- SMC Cluster
  - Node 1
  - Node 2
  - Node 3

- Load balancing with sticky sessions

- Inbound tcp 7600, 8181, 57600
- Outbound tcp 7600, 8181, 57600

- Database Cluster

- Top 1443 or 3306

Copyright © Sophos Limited
Sophos Mobile cluster with Amazon Web Services Cloud

Sophos Mobile

Push services, Apple VPP, Apple App Identifier search, Activation Lock Bypass, Device Enrollment Program, Android Enterprise, ReCaptcha, Intune app protection

Amazon RDS (MySQL or MS SQL)

SMC Cluster (EC2 Instances)

Node 1

Inbound tcp: 7600, 8181, 57600
Inbound udp: 45700
Outbound tcp: 7600, 8181, 57600

Load balancing with sticky sessions

Node 2

Tcp 1433 or 3306
Sophos Secure Email push notifications

1. **Company**
   - Required
   - Trigger

   Exchange Server 2010/2013/2016 with EWS (Exchange Web Services) enabled
   e.g. [https://mail.company.com/ews](https://mail.company.com/ews)
   (same host as for ActiveSync)

2. **https**

3. **Push services**

4. **https/tcp 443**
   - Sends only number of new emails

5. **SSE Push Gateway**
   - push-service.sophosmc.com
Sophos Mobile and Sophos SafeGuard Enterprise keyring synchronization
Sophos Mobile and Microsoft Azure for Intune app protection and federated authentication
4 Ports and protocols

This section lists the communication details for required and optional network connections.

From the internet to the Sophos Mobile server

Port forwarding, NAT, WAF, Reverse Proxy are supported.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>&lt;Sophos Mobile server&gt;</td>
<td>Forwards to HTTPS port</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>&lt;Sophos Mobile server&gt;</td>
<td>Access to Sophos Mobile Admin and Self Service Portal, device sync, UTM, NAC</td>
<td></td>
</tr>
</tbody>
</table>

From the internal network to the Sophos Mobile server

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>&lt;Sophos Mobile server&gt;</td>
<td>Forwards to HTTPS port</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>&lt;Sophos Mobile server&gt;</td>
<td>Access to Sophos Mobile Admin and Self Service Portal, device sync, UTM, NAC</td>
<td></td>
</tr>
</tbody>
</table>

From the Sophos Mobile server to the Internet

Note
A proxy can be used for this traffic. Make sure it can access the APNs servers and keeps the client certificate for services.sophosmc.com intact.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>services.sophosmc.com  (85.22.154.49)</td>
<td>For push notifications to Apple (APNs), Microsoft (MPNS, WNS), Android (Baidu Push) devices</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>android.googleapis.com fcm.googleapis.com/fcm/send</td>
<td>Google Firebase Cloud Messaging for Android devices</td>
<td></td>
</tr>
</tbody>
</table>
### From the Sophos Mobile server to the following internal hosts

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SQL</td>
<td>1433</td>
<td>&lt;your database host&gt;</td>
<td>Only if on a different computer than Sophos Mobile</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>3306</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP plain</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP SSL</td>
<td>465</td>
<td>&lt;your SMTP host&gt;</td>
<td>Enrollment and maintenance emails</td>
<td>Yes</td>
</tr>
<tr>
<td>SMTP TLS</td>
<td>587</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Protocols and Ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>APNs with client cert.</td>
<td>443</td>
<td>api.push.apple.com (17.0.0.0/8)</td>
<td>Apple Push Notification service</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>vpp.itunes.apple.com (17.0.0.0/8)</td>
<td>Apple Volume Purchase Program</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>itunes.apple.com (17.0.0.0/8)</td>
<td>Apple app identifier search</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>deviceservices-external.apple.com (17.0.0.0/8)</td>
<td>Apple Activation Lock Bypass for supervised devices</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>mdmenrollment.apple.com (17.0.0.0/8)</td>
<td>Apple Device Enrollment Program</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>login.live.com *.notify.windows.com</td>
<td>Windows Push Notification service</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td><a href="http://www.googleapis.com">www.googleapis.com</a></td>
<td>Android enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td><a href="http://www.google.com/recaptcha/api/siteverify">www.google.com/recaptcha/api/siteverify</a></td>
<td>Google reCAPTCHA service for password reset and token enrollment</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>login.microsoftonline.com graph.microsoft.com</td>
<td>Intune app protection, federated authentication with Azure AD</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>login.teamviewer.com webapi.teamviewer.com start.teamviewer.com</td>
<td>TeamViewer integration</td>
<td>Yes</td>
</tr>
</tbody>
</table>

From the Sophos Mobile server to the following internal hosts

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SQL</td>
<td>1433</td>
<td>&lt;your database host&gt;</td>
<td>Only if on a different computer than Sophos Mobile</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>3306</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP plain</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP SSL</td>
<td>465</td>
<td>&lt;your SMTP host&gt;</td>
<td>Enrollment and maintenance emails</td>
<td>Yes</td>
</tr>
<tr>
<td>SMTP TLS</td>
<td>587</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### From Android devices to the internet (if connected via Wi-Fi)

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>389</td>
<td>&lt;your LDAP host&gt;</td>
<td>To your directory server</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAPS</td>
<td>636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>&lt;your Exchange server&gt;</td>
<td>For ActiveSync traffic</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>&lt;your SGN server&gt;</td>
<td>For SGN integration</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### From iOS and macOS devices to the internet (if connected via Wi-Fi)

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM</td>
<td>5228-5230</td>
<td>internet (all IP blocks listed in Google’s ASN 15169)</td>
<td>Google Firebase Cloud Messaging (FCM) for Android devices. IP ranges might change regularly. If you use IP restrictions, check the ASN 15169 document at least monthly.</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td><a href="http://www.googleapis.com">www.googleapis.com</a></td>
<td>Zero-touch enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>*.samsungknox.com</td>
<td>Samsung Knox Mobile Enrollment</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.secb2b.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.samsung.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>mesu.apple.com</td>
<td>Apple service for available iOS and macOS updates.</td>
<td>Yes¹</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>push-services.sophosmc.com</td>
<td>Sophos notification service for the Sophos Secure Email iOS app.</td>
<td>Yes²</td>
</tr>
</tbody>
</table>

¹ If not available, Sophos Mobile has no information about iOS and macOS updates. For example, compliance rules regarding mandatory updates have no effect.

² Required to use Exchange Web Services (EWS) notifications. See Sophos knowledge base article 127137.
From Windows and Windows Mobile devices to the internet (if connected via Wi-Fi)

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>*.notify.windows.com</td>
<td>Windows Notification Service (WNS) and Microsoft Push Notification Service (MPNS) for Windows devices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.wns.windows.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>*.notify.live.net</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Between Sophos Mobile server nodes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Comment</th>
<th>Optional?</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>7600, 8181, 57600</td>
<td>&lt;incoming&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>7600, 8181, 57600</td>
<td>&lt;outgoing&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>45700</td>
<td>&lt;incoming&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5 EAS proxy usage scenarios

You use IBM Notes Traveler (formerly IBM Lotus Notes Traveler) for non-iOS devices

The internal EAS proxy is not suitable for this scenario because it only supports the ActiveSync protocol, which is used by Microsoft Exchange and by IBM Notes Traveler for iOS devices. IBM Notes Traveler for non-iOS devices (for example, Android) uses a different protocol that is supported by the standalone EAS proxy.

For non-iOS devices, dedicated Traveler client software is required. This software is available through `<traveler-server>/servlet/traveler` or the Traveler file system. The Install App and Uninstall App features of Sophos Mobile can be used to install and uninstall the Traveler client software. Configuration has to be performed manually.

You want to support multiple backend servers

With the standalone EAS proxy you can set up multiple instances of backend email systems. Each instance needs an incoming TCP port. Each port can connect to a different backend. You need one URL per EAS proxy instance.

You want to set up load balancing for EAS

You can set up standalone EAS proxy instances on several computers and then use a load balancer to distribute the client requests among them.

For this scenario an existing load balancer for HTTP is required.

You want to use client certificate based authentication

For this scenario an existing PKI is required and the public part of the CA certificate has to be set in the EAS proxy.

You need to manage more than 500 devices

For performance reasons, we recommend you use the standalone EAS proxy server instead of the internal version when email traffic for more than 500 client devices must be managed.
6 EAS proxy architecture examples

Learn how to integrate the Sophos Mobile standalone EAS proxy into your organization’s infrastructure. The standalone EAS proxy is available for all installation types of the Sophos Mobile server:

- Sophos Mobile on Premise
- Sophos Mobile as a Service
- Sophos Mobile in Central

### EAS proxy with Sophos Mobile server

<table>
<thead>
<tr>
<th>External URL</th>
<th>Protocol</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://smc.company.com">https://smc.company.com</a></td>
<td>https</td>
<td>ActiveSync server:443</td>
</tr>
<tr>
<td><a href="https://esm.company.com/Microsoft-Sync/ActiveSync">https://esm.company.com/Microsoft-Sync/ActiveSync</a></td>
<td>https</td>
<td>EAS Proxy:443</td>
</tr>
</tbody>
</table>
EAS proxy with Sophos Mobile in Central

<table>
<thead>
<tr>
<th>External URL</th>
<th>Protocol</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://eas.company.com/Microsoft-Server-ActiveSync">https://eas.company.com/Microsoft-Server-ActiveSync</a></td>
<td>https</td>
<td>EAS Proxy:443</td>
</tr>
</tbody>
</table>

Client certificate authorization

<table>
<thead>
<tr>
<th>External URL</th>
<th>Protocol</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://eas.company.com">https://eas.company.com</a></td>
<td>https</td>
<td>EAS Proxy:443</td>
</tr>
<tr>
<td><a href="https://eas.company.com/Microsoft-Server-ActiveSync">https://eas.company.com/Microsoft-Server-ActiveSync</a></td>
<td>https</td>
<td>EAS Proxy:443</td>
</tr>
</tbody>
</table>
Several proxy instances on the same computer

EAS proxy with IBM Traveler clients
EAS proxy behind a load balancer

PowerShell mode

You can set up a PowerShell connection to an Exchange or an Office 365 server. This means that the EAS proxy service communicates with the email server through PowerShell to control the email access for your managed devices. Email traffic is routed directly from the devices to the email server. It is not routed through a proxy.
PowerShell mode (Sophos Mobile in Central)
7 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
8 Legal notices

Copyright © 2019 Sophos Limited. 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, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.