SOPHOS

Cybersecurity made simple.

Sophos Mobile

installation guide

product version: 8.6

Contents

1 About this guide

This guide explains how to install and set up Sophos Mobile version 8.6. It also describes how to update an existing installation of Sophos Mobile.

Unless otherwise noted, all procedures must be performed as an administrator of Microsoft Windows Server or as a user of the relevant group.

2 About Sophos Mobile

Sophos Mobile

Sophos Mobile is the EMM solution for businesses that want to spend less time and effort to manage and secure mobile devices. Manage mobile devices with the easy-to-use, web-based, unified Sophos Central admin interface alongside endpoint, network, or server security from Sophos. Secure container apps and support for mobile OS containerization in iOS, Android enterprise, and Samsung Knox ensure sensitive company data stays separated from personal information on the device.

With its best-in-class data protection, comprehensive security, value-for-money, and flexible management options, Sophos Mobile is the best way to allow the use of mobile devices for work, keeping users productive, business data safe and personal data private.

Sophos Mobile Security

Sophos Mobile Security protects your Android devices without compromising performance or battery life. Powered by leading Sophos anti-malware technology, Sophos Mobile Security offers an award-winning level of antimalware and antivirus protection together with Potentially Unwanted App detection, privacy and security advisors, loss and theft protection, web protection, and much more.

Sophos Secure Workspace

Sophos Secure Workspace is a containerized mobile content management app for iOS and Android that provides a secure way to protect, manage, and distribute business documents and web content. Edit Office format documents without leaving the container environment to ensure encrypted content remains secure. Anti-phishing technology protects users from malicious links in documents and content.

When managed by Sophos Mobile, admins can easily restrict access to content based on device compliance rules. In combination with Sophos SafeGuard Encryption, Sophos Secure Workspace provides seamless exchange of encrypted files—stored locally or in the cloud—between Windows, macOS, iOS and Android users.

Sophos Secure Email

Sophos Secure Email is a fully featured, secure, and containerized email app for Android and iOS that lets you isolate business email, calendar and contacts from private data on a mobile device when managed by Sophos Mobile. All company information is protected with AES-256 encryption and access can easily be revoked based on device compliance rules. Sophos Secure Email also lets IT provision business email securely and consistently across different devices and OS variations.

3 Sophos Mobile licenses

Sophos Mobile offers two types of licenses:

- Mobile Standard license
- Mobile Advanced license

With a license of type Mobile Advanced you can manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.

As a super administrator, you can activate your purchased licenses in the super administrator customer and assign the required number of licensed users to individual customers.

3.1 Trial licenses

Sophos offers a free trial for Sophos Mobile. You can register for the trial on the Sophos website: http://www.sophos.com/en-us/products/free-trials/mobile-control.aspx.

A trial license allows you to manage up to five users and is valid for 30 days.

All you will need when you set up Sophos Mobile for evaluation is the email address you used to register when downloading the installer.

3.2 Upgrade trial licenses to full licenses

To upgrade trial licenses to full licenses you only have to enter your full license key in Sophos Mobile. For further information, see the Sophos Mobile administrator help.

3.3 Update licenses

To update your licenses you have to activate the new license key in Sophos Mobile. For further information, see the Sophos Mobile super administrator guide.

4 Set up Sophos Mobile

This section describes how to install a new Sophos Mobile server. For information on how to update an existing installation, see Update Sophos Mobile (page 23).

4.1 Installation prerequisites

Check the following prerequisites before installing the Sophos Mobile server:

- You have read the Sophos Mobile server deployment guide. This document contains architecture examples for the integration of the Sophos Mobile server into your company's infrastructure, dimensioning guidelines, and a list of required network ports and protocols.
- You have read the Sophos Mobile 8.6 release notes and verified that the computer that hosts the Sophos Mobile server (*server computer*), the devices you want to manage, and other relevant components are supported by Sophos Mobile.
- You have an SSL/TLS certificate for the Sophos Mobile server. See Request an SSL/TLS certificate (page 5).
- No Internet Information Services (IIS) web server or other application using ports 80 or 443 is installed on the server computer.
- The DNS name of the server computer can be resolved over the internet.
- There are one or more LDAP groups containing the users allowed to use the Self Service Portal, if your user accounts are stored in an LDAP directory.

Prerequisites if you want to manage the Sophos Mobile database with an existing database server:

- Microsoft SQL Server or Microsoft SQL Server Express:
  - Windows authentication or SQL Server authentication is used.
  - TCP/IP is turned on.
  - The SQL Server Browser service is enabled.
  - The language of the account used to log in to SQL is set to English.
- Microsoft SQL Server Express:
  - The SQL management tools are installed.

4.2 System environment requirements

The Sophos Mobile installer runs a series of test to verify that your system environment meets all the necessary requirements for Sophos Mobile.

These requirements are:

- You are an administrator on the computer.
- The computer's operating system is supported by Sophos Mobile.
- The computer has at least one network adapter.
- The computer has at least 4 GB of RAM.

- The Microsoft Internet Information Services (IIS) web server is disabled on the computer.
- The following HTTP/S ports are available on the computer: 80, 443, 8080, 8181
- The computer can connect to the Apple Push Notification service (APNs).
- The computer can connect to the Google Firebase Cloud Messaging (FCM) service.
- The computer can connect to the Google reCAPTCHA service.
- The computer can connect to the Windows Push Notification service.
- The computer can connect to the Sophos services.
- Optional: The computer can connect to the Apple Volume Purchase Program (VPP) web service.
- Optional: The computer can connect to the Apple Device Enrollment Program (DEP) web service.
- Optional: The computer can connect to the Apple iTunes web service.
- Optional: The computer can connect to the Apple Activation Lock Bypass web service.
- Optional: The computer can connect to the Google web service for Android enterprise.
- Optional: The computer can connect to the Microsoft web services for Intune app protection.

4.3 Request an SSL/TLS certificate

Your Sophos product delivery includes an SSL Certificate Wizard to request your SSL/TLS certificate for the Sophos Mobile EAS proxy. Run the wizard from the *%MDM_HOME%*`\tools\Wizard` folder, or download it from www.sophos.com/mysophos.

Note
If you use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), the following restrictions apply:

- You must manually install the self-signed certificate or your CA certificate on your devices before you enroll them with Sophos Mobile. If you do not do this, the Sophos Mobile Control app will not trust your server and will refuse to connect. Certificates issued by a globally trusted CA do not require this manual installation.
- You can’t install Android apps from APK files that are hosted on the Sophos Mobile server.
- You can’t use Android zero-touch enrollment or Samsung Knox Mobile Enrollment.

To request your SSL/TLS certificate:

- Start the SSL Certificate Wizard by double-clicking the file *Sophos Mobile SSL Certificate Wizard.exe*.

  The wizard guides you through installation. Enter the required information, considering the following instructions:

  a) On the **Upload CSR** page, you can click the **Open CSR** button to open the CSR file if your certificate vendor supports copy and paste.

  b) On the **Import Certificate Files** page, enter the CA certificate downloaded on the **Upload CSR** page into the **Select CA certificate file** field.

  c) On the **Certificate created** page, the location of the certificate created is shown. You need to refer to this location when setting up Sophos Mobile.

Note
You should create a backup of the folder containing the certificate files.

4.4 Install and set up the Sophos Mobile server

Prerequisites:

- If you plan to connect Sophos Mobile to an existing database, make sure you have the logon credentials for the database available before starting the installation, and that you have sufficient permissions to create new data stores, user accounts and data records.
- If the database is not held locally, you need access to TCP port 1433 (for Microsoft SQL Server) or 3306 (for MySQL). In addition, you need an admin account that the Sophos Mobile server can use to log in to the database.

1. Run the Sophos Mobile installer as administrator, and review and agree to the license agreement.
2. On the **System Property Checks** page, click **Check** to run the tests to verify that your system environment meets all the necessary requirements for Sophos Mobile. See System environment requirements (page 4).

   You can click **Report** to generate a report of the test results.
3. On the **Choose Install Location** page, choose the destination folder for Sophos Mobile server.
4. On the **Database Type Selection** page, select the database type you want to use:
   - **Install and use Microsoft SQL Server Express**: Installs Microsoft SQL Server Express and configures it to be used with Sophos Mobile.
   - **Use existing Microsoft SQL Server installation**: Uses your existing installation of Microsoft SQL Server and creates a new database for Sophos Mobile.
   - **Use existing MySQL installation**: Uses your existing installation of MySQL and creates a new database for Sophos Mobile.
5. On the **Database Settings** page, enter the logon credentials for the database.

   Note
   If you select the **Use SQL Server Authentification** option, you need to make sure that the SQL login language is set to English. See Change the SQL login language (page 9) for details.

6. On the **Database Selection** page, click **Create a new database named** and enter a name for the database to be created, for example SMCDB.
7. On the **Database Configuration** page, progress messages are displayed during the database creation.
   When the database has been successfully created and populated, click **Next** to continue.
8. If you have selected Windows authentication for the database access, there is a page **Set service credentials** where you set the Windows account under which the Sophos Mobile service runs.

   You can use the Local System account or a user account. In the latter case, enter the user account either as `<computer name>\<user name>` or as `<domain>\<user name>`.

   The installer will assign the database access rights to that account.

Note
For security reasons, we recommend that you run the Sophos Mobile service as a user with limited access rights. The user account should have the following properties:

- User account is a local Windows account on the computer on which Sophos Mobile is installed.
- User is not a member of any group, not even of the *users* group.
- User can access your SQL database with the necessary change rights. For an MS-SQL database, this means that the user must be a member of the *db_datareader* and *db_datawriter* roles.

9. On the **Configure super admin account** page, configure the account details of the super administrator.

   The super administrator is primarily intended for customer management and should not be used for routine device management. The super administrator logs in to the super administrator customer and can, for example, predefine settings for new customers and push settings and configurations to existing customers. For further information, see the Sophos Mobile super administrator guide.

   Note
   The super administrator credentials are required for the first login to Sophos Mobile Admin. After installation, additional super administrators can be added in Sophos Mobile Admin.

10. On the **Configure external server name** page, enter a Sophos Mobile server name (for example smc.mycompany.com).

    Note
    The server name must be resolvable by the managed devices.

11. On the **Configure server certificate** page, import a certificate for secure (HTTPS) access to the web server.
    - If you have a trusted certificate, click **Import a certificate from a trusted issuer** and select an option from the drop-down list.
    - If you do not have a trusted certificate yet, select **Create self-signed certificate**.

    Note
    Your Sophos product delivery includes the SSL Certificate Wizard to request your SSL/TLS certificate for Sophos Mobile. See Request an SSL/TLS certificate (page 5).

12. On the next page, enter the relevant certificate information, depending on the type of certificate that you selected.

    Note
    For a self-signed certificate, you need to specify a server that is accessible from the managed devices.

13. On the **Server Information** page, verify the server information, then click **Next** to confirm the server and configuration process.

14. After installation has finished, the **Sophos Mobile Control - Installation finished** dialog box is displayed. Make sure that the **Start Sophos Mobile server now** check box is selected and click **Finish** to start the Sophos Mobile service for the first time.

    Note
    After the service has been started it can take a few minutes before the Sophos Mobile web interface is available.

After the installation there are a few initial configuration steps that you need to perform:

- Configure the Sophos Mobile web server to only accept requests directed to your domain name. See Configure the Sophos Mobile web server (page 8).
- Log in to Sophos Mobile Admin for the first time to start the **First steps** wizard. See the Sophos Mobile startup guide.
- For iOS devices, you need to get an Apple Push Notification service certificate. See the Sophos Mobile startup guide.
- Optionally, you can set up a standalone EAS proxy for email filtering. See Standalone EAS proxy (page 10).

4.5 Configure the Sophos Mobile web server

Sophos Mobile includes a web server component for providing the content of the Sophos Mobile Admin and Self Service Portal web applications. You can configure the web server to adjust it to your environment.

Requests to a web server include a Host field in the request header, specifying the web application to process the request. An attacker can potentially manipulate the value of that Host field to provoke unintended behavior.

After installation, the web server component of Sophos Mobile doesn't verify the value of the Host field. We recommend you configure the web server so that it only accepts requests directed to your domain name.

1. On the computer on which you've installed the Sophos Mobile server, run the script *%MDM_HOME%*`\tools\HostValidationUndertowFilter\addModule.bat`

   Replace *%MDM_HOME%* by your Sophos Mobile installation folder.
2. Open the file *%MDM_HOME%*`\wildfly\standalone\configuration\smc-config.xml` in a text editor and search for the following section:

   ```
   <filter name="hostheadervalidation" ...>
       <param name="allowedHosts" value="localhost"/>
   </filter>
   ```
3. After `localhost`, add your domain name for Sophos Mobile Admin and for the Self Service Portal.

   For example if your domain name is `smc.example.com`, change the line as follows:

   ```
   <param name="allowedHosts" value="localhost,smc.example.com"/>
   ```

   If your Sophos Mobile server can be accessed under more than one domain name, enter all names separated by commas.
4. Save the file `smc-config.xml`
5. Restart the Sophos Mobile service.

4.6 Change the SQL login language

If you have configured the Sophos Mobile server to use SQL Server authentication to connect to the database, the SQL login language must be set to English. Otherwise, an error occurs when the Sophos Mobile service is started.

This topic describes how to change the SQL login language to English.

1. Stop the Sophos Mobile service.
2. Open SQL Server Management Studio on the server and select **Security > Logins**.
3. On the **General** page of the **Login Properties**, set **Default language** to English, then click **OK** to save the changes.
4. Restart the Sophos Mobile service.

5 Standalone EAS proxy

You can set up an EAS proxy to control the access of your managed devices to an email server. Email traffic of your managed devices is routed through that proxy. You can block email access for devices, for example a device that violates a compliance rule.

The devices must be configured to use the EAS proxy as email server for incoming and outgoing emails. The EAS proxy will only forward traffic to the actual email server if the device is known in Sophos Mobile and matches the required policies. This guarantees higher security as the email server does not need to be accessible from the Internet and only devices that are authorized (correctly configured, for example with passcode guidelines) can access it. Also, you can configure the EAS proxy to block access from specific devices.

There are two types of EAS proxy:

- The internal EAS proxy that is automatically installed with Sophos Mobile. It supports incoming ActiveSync traffic as used by Microsoft Exchange or IBM Notes Traveler for iOS and Samsung Knox devices.
- A standalone EAS proxy that can be downloaded and installed separately. It communicates with the Sophos Mobile server through an HTTPS web interface.

Note
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.

Note
Because macOS doesn't support the ActiveSync protocol, you can't use the internal or the standalone EAS proxy to filter email traffic coming from Macs.

Features

The standalone EAS proxy has additional features compared to the internal version:

- Support for IBM Notes Traveler for non-iOS devices (for example, Android). The Traveler client for these devices uses a protocol (not ActiveSync) that is not supported by the internal EAS proxy.
- Support for multiple Microsoft Exchange or IBM Notes Traveler email servers. You can set up one EAS proxy instance per email server.
- Load balancer support. You can set up standalone EAS proxy instances on several computers and then use a load balancer to distribute the client requests among them.
- Support for certificate-based client authentication. You can select a certificate from a certification authority (CA), from which the client certificates must be derived.
- Support for email access control through PowerShell. In this scenario, the EAS proxy service communicates with the email server through PowerShell to control the email access of your managed devices. Email traffic happens directly from the devices to the email server and is not routed through a proxy. See Set up email access control through PowerShell (page 15).
- The EAS proxy remembers the device status for 24 hours. If the Sophos Mobile server is offline, for example during an update, email traffic is filtered based on the last known device status. After 24 hours, all email traffic is blocked.

Note
For non-iOS devices, filtering abilities of the standalone EAS proxy are limited due to the specifics of the IBM Notes Traveler protocol. Traveler clients on non-iOS devices do not send the device ID with every request. Requests without a device ID are still forwarded to the Traveler server, even though the EAS proxy is not able to verify that the device is authorized.

5.1 Usage scenarios for the standalone EAS proxy

Note
Additional to the information provided in this section, the Sophos Mobile server deployment guide contains schematic diagrams for the integration of the standalone EAS proxy into your company's infrastructure. We recommend that you read the information before performing the installation and deployment of the standalone EAS proxy.

A standalone EAS proxy server should be used for the following 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.

5.2 Download the EAS proxy installer

1. Log in to Sophos Mobile Admin as super administrator.
2. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
3. Under **External**, click the link to download the EAS proxy installer.

The installer file is saved to your local computer.

5.3 Install the standalone EAS proxy

Prerequisites:

- Sophos Mobile has been installed and set up.
- All required email servers are accessible. The EAS proxy installer will not configure connections to servers that are not available.
- You are an administrator on the computer where you install the EAS proxy.

Note
The Sophos Mobile server deployment guide contains schematic diagrams for the integration of the standalone EAS proxy into your company's infrastructure. We recommend that you read the information before performing the installation and deployment of the standalone EAS proxy.

1. Run `Sophos Mobile EAS Proxy Setup.exe` to start the **Sophos Mobile EAS Proxy - Setup Wizard**.
2. On the **Choose Install Location** page, choose the destination folder and click **Install** to start installation.
   After the installation has been completed, the **Sophos Mobile EAS Proxy - Configuration Wizard** is started automatically and guides you through the configuration steps.
3. In the **Sophos Mobile server configuration** dialog, enter the URL of the SMC server that the EAS proxy will connect with.

   You should also select **Use SSL for incoming connections (Clients to EAS Proxy)** to secure the communication between clients and the EAS proxy.

   Optionally, select **Use client certificates for authentication** if you want the clients to use a certificate in addition to the EAS proxy credentials for authentication. This adds an additional layer of security to the connection.

   Select **Allow all certificates** if your Sophos Mobile server presents varying certificates to the EAS proxy, for example because there are several server instances behind a load balancer, and each instance uses a different certificate. When this option is selected, the EAS proxy will accept any certificate from the Sophos Mobile server.

Important
Because the **Allow all certificates** option reduces the security level of the server communication, we strongly recommend that you select it only if required by your network environment.

4. If you selected **Use SSL for incoming connections (Clients to EAS Proxy)** before, the **Configure server certificate** page is displayed. On this page you create or import a certificate for the secure (HTTPS) access to the EAS proxy.

   Note
   Your Sophos product delivery includes the SSL Certificate Wizard to request your SSL/TLS certificate for the Sophos Mobile EAS proxy. For further information, see Request an SSL/TLS certificate (page 5).

   - If you do not have a trusted certificate yet, select **Create self-signed certificate**.
   - If you have a trusted certificate, click **Import a certificate from a trusted issuer** and select one of the following options from the list:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. On the next page, enter the relevant certificate information, depending on the type of certificate that you selected.

   Note
   For a self-signed certificate, you need to specify a server that is accessible from the client devices.

6. If you selected **Use client certificates for authentication** before, the **SMC client authentication configuration** page is displayed. On this page, you select a certificate from a certification authority (CA), from which the client certificates must be derived.

   When a client tries to connect, the EAS proxy will check if the client certificate is derived from the CA that you specify here.
7. On the **EAS Proxy instance setup** page, configure one or more EAS proxy instances.
   - **Instance type**: Select **EAS proxy**.
   - **Instance name**: A name to identify the instance.
   - **Server port**: The port of the EAS proxy for incoming email traffic. If you set up more than one proxy instance, each of these must use a different port.
   - **Require client certificate authentication**: Email clients must authenticate themselves when connecting to the EAS proxy.
   - **ActiveSync server**: The name or IP address of the Exchange ActiveSync Server instance with which the proxy instance will connect.
   - **SSL**: Communication between the proxy instance and Exchange ActiveSync Server is secured by SSL or TLS (depending on what the server supports).
   - **Allow EWS subscription requests from Secure Email**: Select this to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email.

Note

— By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this check box, subscription requests are allowed. Other requests remain blocked.

— For information on how to configure EWS for your Exchange server, see Sophos knowledge base article 127137.

- **Enable Traveler client access**: Only select this check box if you need to allow access by IBM Notes Traveler clients on non-iOS devices.

8. After entering the instance information, click **Add** to add the instance to the **Instances** list.

   For every proxy instance, the installer creates a certificate that you need to upload to the Sophos Mobile server. After you have clicked **Add**, a message window opens, explaining how to upload the certificate.

9. In the message window, click **OK**.
   This will open a dialog, showing the folder in which the certificate has been created.

   Note
   You can also open the dialog by selecting the relevant instance and clicking the **Export config and upload to Sophos Mobile server** link on the **EAS Proxy instance setup** page.

10. Make a note of the certificate folder. You need this information when you upload the certificate to Sophos Mobile.
11. Optional: Click **Add** again to configure additional EAS proxy instances.
12. When you have configured all required EAS proxy instances, click **Next**.
    The server ports that you entered are tested and inbound rules for the Windows Firewall are configured.
13. On the **Allowed mail user agents** page, you can specify mail user agents (i.e. email client applications) that are allowed to connect to the EAS proxy. When a client connects to the EAS proxy using an email application that is not specified, the request will be rejected.

    - Select **Allow all mail user agents** to configure no restriction.
    - Select **Only allow the specified mail user agents** and then select a mail user agent from the list. Click **Add** to add the entry to the list of allowed agents. Repeat this for all mail user agents that are allowed to connect to the EAS proxy.

14. On the **Sophos Mobile EAS Proxy - Configuration Wizard finished** page, click **Finish** to close the Configuration Wizard and return to the Setup Wizard.
15. In the Setup Wizard, make sure that the **Start Sophos Mobile EAS Proxy server now** check box is selected, then click **Finish** to complete the configuration and to start the Sophos Mobile EAS proxy for the first time.

To complete the EAS proxy configuration, upload the certificates that were created for every proxy instance to Sophos Mobile:

16. Log in to Sophos Mobile Admin as a super administrator.
17. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
18. Under **External**, click **Upload a file**. Upload the certificate that the setup wizard created for the PowerShell connection.

    If you have set up more than one instance, repeat this for all instance certificates.

19. Click **Save**.

20. In Windows, open the **Services** dialog and restart the **EASProxy** service.
21. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
22. Under **External**, click **Upload a file**. Upload the certificate that the setup wizard created for the PowerShell connection.

    If you have set up more than one instance, repeat this for all instance certificates.
23. Click **Save**.
24. In Windows, open the **Services** dialog and restart the **EASProxy** service.

This completes the initial setup of the standalone EAS proxy.

Note
Every day, the EAS proxy log entries are moved to a new file, using the naming pattern `EASProxy.log.yyyy-mm-dd`. These daily log files are not deleted automatically and thus may cause disk space issues over time. We recommend that you set up a process to move the log files to a backup location.

5.4 Set up email access control through PowerShell

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.

Note
For a schematic of the PowerShell communication, see the Sophos Mobile server deployment guide.

Note
Because macOS doesn't support the ActiveSync protocol, you can't use PowerShell to control email access by Macs.

The PowerShell scenario has these advantages:

- Devices communicate directly with the Exchange server.
- You do not need to open a port on your server for incoming email traffic from your managed devices.

Supported email servers are:

- Exchange Server 2013
- Exchange Server 2016
- Office 365 with an Exchange Online plan

To set up PowerShell:

1. Configure PowerShell.
2. Create a service account on the Exchange server or in Office 365. This account is used by Sophos Mobile to execute PowerShell commands.

3. Set up one or more PowerShell connection instances to Exchange or Office 365.
4. Upload the instance certificates to Sophos Mobile.

Configure PowerShell

1. On the computer on which you are going to install the EAS proxy, open Windows PowerShell, as an administrator, and enter:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Note
If PowerShell is not available, install it as described in the Microsoft article Installing Windows PowerShell (external link).

2. If you want to connect to a local Exchange server, open Windows PowerShell as administrator on that computer and enter the same command as before:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Note
This step is not required for Office 365.

Create a service account

3. Log in to the relevant admin console:
   - For Exchange Server 2013/2016: **Exchange Admin Center**
   - For Office 365: **Office 365 Admin Center**
4. Create a user account. This account is used as a service account by Sophos Mobile to execute PowerShell commands.
   - Use a user name like `smc_powershell` that identifies the account purpose.
   - Turn off the setting to make the user change their password the next time they log in.
   - Remove any Office 365 license that was automatically assigned to the new account. Service accounts don't require a license.
5. Create a new role group and assign it the required permissions.
   - Use a role group name like `smc_powershell`.
   - Add the **Mail Recipients** and **Organization Client Access** roles.
   - Add the service account as a member.

Set up PowerShell connections

6. Use the setup wizard as if you would set up a standalone EAS Proxy. On wizard page **EAS Proxy instance setup**, configure the following settings:
   - **Instance type**: Select **PowerShell Exchange/Office 365**.
   - **Instance name**: A name to identify the instance.
   - **Exchange server**: The name or IP address of the Exchange server (for a local Exchange server installation) or `outlook.office365.com` (for Office 365). Don't include a prefix `https://` or a suffix `/powershell`. These are added automatically.
   - **Allow all certificates**: The certificate that the Exchange server presents is not verified. Use this for example if you have a self-signed certificate installed on your Exchange

server. Because the **Allow all certificates** option reduces the security level of the server communication, we strongly recommend that you select it only if required by your network environment.

- **Allow EWS subscription requests from Secure Email**: Select this to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email.

  Note
  - By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this check box, subscription requests are allowed. Other requests remain blocked.
  - For information on how to configure EWS for your Exchange server, see Sophos knowledge base article 127137.

- **Service account**: The name of the user account you created in the Exchange or Office 365 admin console.
- **Password**: The password of the user account.

7. Click **Add** to add the instance to the **Instances** list.
8. **Optional:** Repeat the previous steps to set up PowerShell connections to other Exchange or Office 365 servers.
9. Complete the setup wizard as described in Install the standalone EAS proxy (page 12).

Upload certificates

10. Log in to Sophos Mobile Admin as a super administrator.
11. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
12. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.

    This prevents other email apps from connecting to your email server.
13. Under **External**, click **Upload a file**. Upload the certificate that the setup wizard created for the PowerShell connection.

    If you have set up more than one instance, repeat this for all instance certificates.
14. Click **Save**.
15. In Windows, open the **Services** dialog and restart the **EASProxy** service.

This completes the initial setup of PowerShell connections. Email traffic between a managed device and the Exchange or Office 365 servers is blocked if the device violates a compliance rule. You can block an individual device by setting the email access mode for that device to **Deny**.

Note
Depending on the configuration of your Exchange server, devices receive a notification when their email access is blocked.

6 Load balancing and high availability

Sophos Mobile makes it possible to set up a high-availability environment. This ensures that the SMC service remains externally accessible and tasks can be further processed even after failure of a Sophos Mobile server node. To achieve this, load balancing, that distributes client and browser sessions by using DNS Round Robin to the available nodes, is required.

The following describes setting up clustering for Sophos Mobile and configuring load balancing with Sophos UTM.

6.1 Requirements

- One separate Windows server for each Sophos Mobile server node.
- All nodes must be on the same network.
- One Microsoft SQL or MySQL database server or cluster.
- Sophos UTM or Apache Reverse Proxy (mod_proxy) for load balancing. Load balancer must support permanent session cookies and official SSL/TLS web server certificates.

Note
For detailed information about the installation requirements see the Sophos Mobile 8.6 release notes.

Architecture

For an example of a three-node Sophos Mobile cluster see the Sophos Mobile server deployment guide.

For multicast communication between the individual Sophos Mobile server nodes, optionally a separate network can be used. The network interface to be used can be selected during cluster configuration, as described in Set up the first node (page 19). It may also be a VLAN.

Note
If you want to operate a second Sophos Mobile cluster for test purposes, a separate network is needed.

Ports and protocols

The following table shows the required ports and protocols for communication between the individual nodes of a Sophos Mobile server cluster.

Protocol	Ports	Destination
TCP	7600, 8181, 57600	*<Incoming>*

Protocol	Ports	Destination
TCP	7600, 8181, 57600	*<Outgoing>*
UDP	45700	*<Incoming>*

Server certificates

When you set up Sophos Mobile, you configure an SSL/TLS web server certificate that allows the Sophos Mobile Control app to establish a secure connection to the Sophos Mobile server. We recommend that you use a certificate that is issued by a globally trusted certificate authority (CA). In a clustered environment with several Sophos Mobile server nodes behind a load balancer, this might not be practical. You might want to use a self-signed certificate instead.

Note
If you use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), the following restrictions apply:

- You must manually install the self-signed certificate or your CA certificate on your devices before you enroll them with Sophos Mobile. If you do not do this, the Sophos Mobile Control app will not trust your server and will refuse to connect. Certificates issued by a globally trusted CA do not require this manual installation.
- You can't install Android apps from APK files that are hosted on the Sophos Mobile server.
- You can't use Android zero-touch enrollment or Samsung Knox Mobile Enrollment.

6.2 Set up cluster nodes

To set up a clustered environment you install the first node as described in Install and set up the Sophos Mobile server (page 6). Clustering itself is then activated using the **Configuration Wizard**.

For all other nodes, the database created during installation of the first node has to be selected and clustering has to be activated.

Note
It is also possible to configure an existing SMC server for clustering and to extend the environment by adding additional nodes.

6.2.1 Set up the first node

1. Install Sophos Mobile as described in Install and set up the Sophos Mobile server (page 6) and write down the name of the database you created. Specify this database when installing further nodes.
2. At the end of the installation deselect the **Start Sophos Mobile server now** option in the **Sophos Mobile - Installation finished** dialog.

Note
If the Sophos Mobile service has already been started it will automatically be stopped and restarted during the configuration described later in this section. Alternatively, you can manually stop the service from the menu of the Sophos Mobile system tray icon.

3. On the server, click **Start**, go to **Sophos Mobile** and click **SMC Configuration Wizard**.
4. The **Welcome** page of the Sophos Mobile Configuration Wizard is displayed. Click **Next**.
5. On the **Database Selection** page, select **Skip database configuration** and click **Next**.
6. On the **Choose configuration steps** page, select **Configure cluster support** and click **Next**.
7. On the **Cluster Configuration** page, use the drop-down list of available network interfaces to select the interface that will be used for multicast communication between the server node that you are about to set up and the other nodes.
8. Click through the remaining pages of the configuration wizard. Make sure that you click **Yes** when asked to start the SMC service.
   The configuration of the first SMC server node is now complete. Click **Finish** in the **Sophos Mobile - Configuration Wizard finished** dialog.

6.2.2 Set up further nodes

1. Start the installation of Sophos Mobile as described in Install and set up the Sophos Mobile server (page 6).
2. On the **Database selection** page, select the database you created when you installed the first node and click **Next**.

   The **Database configuration** dialog box is displayed. It shows the progress of the configuration process.
3. On the **Database configuration** page, wait until the configuration process has finished, then click **Next**.
4. On the **Choose configuration steps** page, select **Configure cluster support** and click **Next**.
5. On the **Configure server certificate** page, create a self-signed certificate as described in Install and set up the Sophos Mobile server (page 6) and click **Next**.
6. On the **Cluster Configuration** page, use the drop-down list of available network interfaces to select the interface of the Sophos Mobile server node that you are about to set up, then click **Next**.
7. Click through the remaining pages of the configuration wizard. On the **Sophos Mobile - Installation finished** page, select **Start Sophos Mobile server now** to start the cluster node that you just configured.
8. If you've configured the web server component of Sophos Mobile on the first node to only accept requests directed to your domain name, repeat this for all other nodes. See Configure the Sophos Mobile web server (page 8).

If required, repeat this procedure to configure additional nodes.

6.3 Set up load balancing with Sophos UTM

This topic describes how to set up Sophos UTM as a load balancer for a cluster of Sophos Mobile server nodes. For more information on configuring Sophos UTM, see the Sophos UTM documentation.

Note

- In order to use Sophos UTM for clustering you need a Sophos UTM license with a **Sophos Webserver Protection** subscription.
- As described later in this section, you need to specify a certificate to protect the communication between the managed devices and the virtual web server that you set up in Sophos UTM. For simplicity, we recommend that you use the same certificate that you used for the Sophos Mobile server (see Request an SSL/TLS certificate (page 5)). If you used a self-signed certificate, it is mandatory that you use that same certificate.

1. Log into Sophos UTM WebAdmin.
2. From the WebAdmin menu section **Webserver Protection**, go to the **Web Application Firewall > Real Webservers** tab.
3. Click **New Real Webserver** to create an SMC node.
4. In the **Add Real Webserver** dialog, enter the following settings:
   a) **Name**: Enter a descriptive name for the web server (for example `SMC node`).
   b) **Host**: Select or add a host. Select a host by clicking the folder symbol next to the **Host** field. Drag a host from the list of available hosts into the **Host** field.
      For additional information on how to add a definition, see the topic *Network Definitions* in the UTM Administration Guide.
   c) **Type**: Select **Encrypted (HTTPS)**.

   Click **Save** to save the configuration.

   Repeat the previous step for each Sophos Mobile server node.
5. From the WebAdmin menu section **Webserver Protection**, go to the **Certificate Management > Certificates** tab.
6. Click **New Certificate** to upload an SSL/TLS web server certificate.
7. In the **Add Certificate** dialog, enter the following settings:
   a) **Name**: Enter a descriptive name for the certificate.
   b) **Method**: Select **Upload**.
   c) **File type**: Select **PKCS#12(Cert+CA)**
   d) **Password**: Enter the password for your certificate file.
   e) **File**: Click the folder icon next to the **File** box, select the certificate you want to upload and click **Start Upload**.

   Click **Save** to save the configuration. The certificate is added to the **Certificates** list.
8. From the WebAdmin menu section **Webserver Protection**, go to the **Web Application Firewall > Virtual Webservers** tab.
9. Click **New Virtual Webserver** to add a virtual web server for the cluster.
10. In the **Add Virtual Webserver** dialog box, make the following settings:
    a) **Name**: Enter a descriptive name for the virtual web server (for example `SMC cluster`).
    b) In the **Interface** list, select the WAN interface over which the cluster should be accessible from outside.
    c) **Type**: Select **Encrypted (HTTPS) & redirect**.
    d) In the **Certificate** list, select the web server's certificate you uploaded beforehand.

e) **Domains** (only with wildcard certificate, that is a public key certificate that can be used with multiple subdomains): Enter the domains the web server is responsible for, for example `shop.example.com`, or use the **Action** icon to import a list of domain names.

Domains must be entered as fully qualified domain names (FQDN).

You can use an asterisk (*) as a wildcard for the domain prefix, for example, `*.mydomain.com`. Domains with wildcards are considered as fallback settings: The virtual web server with the wildcard domain entry is only used when no other virtual web server with a more specific domain name is configured.

Example: A client request to `a.b.c` will match `a.b.c` before `*.b.c` before `*.c`.

f) **Real Webservers**: Select the SMC nodes you created beforehand.

Important
Do not select a firewall profile.

Click **Save** to save the configuration. The server is added to the **Virtual Webservers** list.

11. Enable the virtual web server.

    The new virtual web server is disabled by default. Click the toggle switch to enable the virtual web server. The toggle switch color should change from gray (disabled) to green (enabled).

12. Go to the **Site Path Routing** tab.
13. In the **Virtual Webservers** list, go to the virtual web server you added and click **Edit**.
14. In the **Edit Site Path Route** dialog box, click **Advanced** and select **Enable sticky session cookie**. Click **Save** to save the configuration.

7 Update Sophos Mobile

Sophos Mobile server installations can be updated directly from versions 8, 8.1 or 8.5 to 8.6.

Older versions need to be updated to version 8 beforehand. For details, see the Sophos Mobile 8 documentation.

7.1 Update Sophos Mobile server

To update your Sophos Mobile server installation to version 8.6, start the Sophos Mobile 8.6 installer and follow the instructions. The installer automatically detects if an existing installation needs to be updated to version 8.6.

A system property check will be performed before the update starts. If all checks are passed you can proceed with the update. Database and files will be updated automatically without any user interaction. Once the update is complete, the Sophos Mobile service will be started again.

Note
If you used Windows Authentication during your initial Sophos Mobile server installation the **Start Sophos Mobile server now** option is grayed out. You have to start the service manually.

7.2 Post-update tasks

7.2.1 Re-configure the Sophos Mobile web server

If you've configured the web server component of Sophos Mobile to only accept requests directed to your domain name, you must repeat this step after you've updated Sophos Mobile. See Configure the Sophos Mobile web server (page 8).

7.2.2 Re-configure Self Service Portal enrollment for Windows computers

If you've configured Self Service Portal enrollment for Windows computers, you must adjust the configuration after you've updated Sophos Mobile from version 8 to version 8.6. In Sophos Mobile 8, the initial package is a policy while in Sophos Mobile 8.1 and later it is a task bundle.

In Sophos Mobile Admin, perform the following steps:

1. Under **Task bundles > Windows**, create a new task bundle containing an **Enroll** task and, optionally, one or more **Assign policy** and/or **Install app** tasks.

   If required, create different task bundles for corporate and personal computers.
2. Under **Setup > Self Service Portal > Group settings**, select the task bundles as initial packages for the **Windows** platform and then click the check box next to **Windows**.

For further information on task bundles and Self Service Portal settings, see the Sophos Mobile administrator help.

7.3 Update a server cluster

When updating a cluster of Sophos Mobile server nodes, it is important that all nodes are running on the same version at all times, and that the server version matches the database version. To do this:

1. Shut down all server nodes by stopping the Sophos Mobile service on the relevant computers.
2. Update the first node as described in Update Sophos Mobile server (page 23).
   This also updates the database.
3. Start the updated server node and check that the update was successful.
4. Update the remaining server nodes.

Tip
If you are using the standalone EAS proxy, your managed devices can access your email server even when all Sophos Mobile server nodes are stopped. This is because the EAS proxy caches the device status for up to 60 minutes when not connected to the Sophos Mobile server.

7.4 Update standalone EAS proxy

To update your standalone EAS proxy, run the EAS proxy installer and follow the instructions. The installer automatically detects if an existing installation needs to be updated.

If you are using a cluster of EAS proxy server nodes behind a load balancer, you can update these nodes independently of each other and in any sequence.

Tip
Do not stop all EAS proxy server nodes at the same time. This makes sure that email communication of your managed devices is not interrupted during the update.

8 Technical reference

8.1 Sophos Mobile server features

The core component of the Sophos Mobile product is the Sophos Mobile server. Its main features include:

- The server is connected to the Internet.
- The server makes it possible to set up a high-availability environment.
- The administrator controls the server using the web interface.
- End users can register their devices by using the Self Service Portal, or get a device from the administrator that has already been prepared for auto-enrollment.
- The managed devices synchronize with the server through HTTPS.
- You can use an existing Microsoft SQL Server or MySQL database to store device and application information. Alternatively, you can let the Sophos Mobile installer create a new database using Microsoft SQL Server Express.
- The database can reside on the same or a separate computer. This allows the use of database clusters.
- The server supports multi-tenant setups to allow different customers on the same server.
- Email access is possible through an integrated or a standalone EAS proxy. For the standalone variant, HTTPS access to the SMC server is required.

The Sophos Mobile server has been developed for Java EE (Enterprise Edition). It installs and runs in the well-tested industry-standard WildFly application server.

The server may be installed in virtualized environments.

8.2 Sophos Mobile web interfaces

8.2.1 Sophos Mobile administration interface

Sophos Mobile is managed through a web interface that is secured by a login and a session mechanism. You can implement password policies. Access control allows different user roles. These roles have different sets of access rights. Each user can be assigned exactly one role.

For further information, see the Sophos Mobile administrator help.

8.2.2 Super administrator interface

The super administrator is primarily used to set up and manage customers for device management. The first super administrator account is created during Sophos Mobile setup. See Install and set up the Sophos Mobile server (page 6).

As a super administrator you log in to the super administrator customer which is also created during Sophos Mobile setup. For the super administrator customer, Sophos Mobile Admin shows a customized view for super administrator tasks.

8.2.3 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 Sophos Mobile administrator and can be associated with any tenant. The Self Service Portal is designed for end users to register their devices with Sophos Mobile. 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 platform and configuration. As an administrator you can configure the Self Service Portal functions available to end users.

For information on how to configure the Self Service Portal for end users, see the Sophos Mobile administrator help.

9 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.
- Visit the Sophos Support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

10 Legal notices