## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this document</td>
<td>1</td>
</tr>
<tr>
<td>What are the key steps?</td>
<td>2</td>
</tr>
<tr>
<td>Activate Mobile Advanced licenses</td>
<td>3</td>
</tr>
<tr>
<td>Configure settings</td>
<td>4</td>
</tr>
<tr>
<td>Configure personal settings</td>
<td>4</td>
</tr>
<tr>
<td>Configure IT contact</td>
<td>4</td>
</tr>
<tr>
<td>Set Android management mode</td>
<td>6</td>
</tr>
<tr>
<td>Set up Android Enterprise - Overview</td>
<td>6</td>
</tr>
<tr>
<td>Set up Android Enterprise (Managed Google Play Account scenario)</td>
<td>6</td>
</tr>
<tr>
<td>Apple Push Notification service certificates</td>
<td>8</td>
</tr>
<tr>
<td>Create APNs certificate</td>
<td>8</td>
</tr>
<tr>
<td>Standalone EAS proxy</td>
<td>9</td>
</tr>
<tr>
<td>Download the EAS proxy installer</td>
<td>10</td>
</tr>
<tr>
<td>Install the standalone EAS proxy</td>
<td>10</td>
</tr>
<tr>
<td>Set up email access control through PowerShell</td>
<td>13</td>
</tr>
<tr>
<td>Block email access for unmanaged devices</td>
<td>15</td>
</tr>
<tr>
<td>Configure a connection to the standalone EAS proxy server</td>
<td>16</td>
</tr>
<tr>
<td>Determine the Sophos Mobile server URL</td>
<td>17</td>
</tr>
<tr>
<td>Compliance policies</td>
<td>18</td>
</tr>
<tr>
<td>Create compliance policy</td>
<td>18</td>
</tr>
<tr>
<td>Device groups</td>
<td>20</td>
</tr>
<tr>
<td>Create device group</td>
<td>20</td>
</tr>
<tr>
<td>Get started with device policies</td>
<td>21</td>
</tr>
<tr>
<td>Create task bundle for Android devices</td>
<td>22</td>
</tr>
<tr>
<td>Create task bundle for iPhones and iPads</td>
<td>23</td>
</tr>
<tr>
<td>Create Self Service Portal configurations</td>
<td>24</td>
</tr>
<tr>
<td>Test device enrollment through the Self Service Portal</td>
<td>26</td>
</tr>
<tr>
<td>Use the <strong>Add device</strong> wizard</td>
<td>27</td>
</tr>
<tr>
<td>Glossary</td>
<td>29</td>
</tr>
<tr>
<td>Support</td>
<td>31</td>
</tr>
<tr>
<td>Legal notices</td>
<td>32</td>
</tr>
</tbody>
</table>

(2020/06/05)
1 About this document

This document explains how to set up Sophos Mobile step by step to manage your devices.
The descriptions apply to the Sophos Mobile product in Sophos Central.
For other versions of this document, see the Sophos Mobile documentation web page.
2 What are the key steps?

To start using Sophos Mobile:

2. Configure personal settings, technical support contact details, and settings for the Self Service Portal.
3. Upload an Apple Push Notification service certificate to manage iPhones, iPads, and Macs.
4. Optional: Set up a standalone EAS proxy to filter email traffic from the managed devices to an email server.
5. Create compliance policies.
6. Create device groups.
7. Configure devices.
9. Test device enrollment in the Self Service Portal.
3 Activate Mobile Advanced licenses

With Mobile Advanced licenses you can use Sophos Mobile to manage Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.

You activate Mobile Advanced licenses in Sophos Central Admin:

In Sophos Central Admin, click your account name (upper right of the user interface), select Licensing and then enter your license key in the Apply Activation Code field.

When the key is activated, the license details are displayed.
4 Configure settings

Configure the following settings:
- Personal settings, for example the platforms you want to manage
- Technical support contact details
- Self Service Portal settings

4.1 Configure personal settings

You can adjust the appearance of Sophos Mobile Admin to your personal preferences. For example, you can set the language, the time zone, or the visible device platforms.

Note
These settings only affect the administrator account you're currently signed in with.

1. On the menu sidebar, under SETTINGS, click Setup > General, and then click the Personal tab.
2. Configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time zone</td>
<td>The time zone in which dates are shown.</td>
</tr>
<tr>
<td>Unit system</td>
<td>The unit system for lengths (Metric or Imperial).</td>
</tr>
<tr>
<td>Lines per page in tables</td>
<td>The maximum number of entries displayed per table page.</td>
</tr>
<tr>
<td>Expert mode</td>
<td>This setting turns on additional features:</td>
</tr>
<tr>
<td></td>
<td>• The Show device page includes the Custom properties tab with your custom device properties.</td>
</tr>
<tr>
<td></td>
<td>• The Show device page includes the Internal properties tab with additional properties the device reports.</td>
</tr>
<tr>
<td></td>
<td>• Several policy configuration pages include the Extra settings section to configure optional settings.</td>
</tr>
<tr>
<td>Activated platforms</td>
<td>The device platforms you want to view.</td>
</tr>
<tr>
<td></td>
<td>In Sophos Mobile Admin, only pages and settings relevant for the selected platforms are shown.</td>
</tr>
</tbody>
</table>

3. Click Save.

4.2 Configure IT contact

Provide your IT contact details so that users can get help with questions or problems.

The information you enter here is displayed on the users’ devices.
1. On the menu sidebar, under **Settings**, click **Setup > General**, and then click the **IT contact** tab.
2. Enter the contact information.
3. Click **Save**.
5 Set Android management mode

For Android devices, you can choose between the Android Enterprise and Device administrator (legacy feature) management modes.

To set the Android management mode, do as follows:
1. On the menu sidebar, under SETTINGS, select Setup > Android setup and then the Android tab.
2. In Management mode, select Android Enterprise.
3. Click Save.

Next, set up Android Enterprise for your organization.

5.1 Set up Android Enterprise - Overview

To set up Android Enterprise for your organization, you can choose between different scenarios. The Managed Google Play Account scenario is the easiest method to set up Android Enterprise and is described in this document.

For details on other Android Enterprise scenarios, see the Sophos Mobile administrator help.

Related information
Sophos Mobile administrator help

5.2 Set up Android Enterprise (Managed Google Play Account scenario)

Sophos Mobile guides you through the procedure to set up Android Enterprise for your organization.
1. On the menu sidebar, under SETTINGS, select Setup > Android setup and then the Android Enterprise tab.
2. Select Configure.
3. Select “Managed Google Play Account” scenario and then Next.
4. Select Register account.
   This redirects you to a Google website where you register your organization with Android Enterprise.
5. Sign in to the Google website with your Google account.

Note
We recommend that you create a new Google account for this purpose.

6. On the Google website, follow the steps to register your organization.
**Tip**
When specifying your organization name, we recommend that you include the term **Sophos Mobile**. For example:

Organization name (Sophos Mobile)

After you have completed the registration steps, the Google website redirects you back to Sophos Mobile.

7. In Sophos Mobile, select **Finalize setup** to complete the registration process.
6 Apple Push Notification service certificates

To use the built-in Mobile Device Management (MDM) protocol of iPhones, iPads, and Macs, Sophos Mobile must use the Apple Push Notification service (APNs) to trigger the devices.

APNs certificates have a validity period of one year.

6.1 Create APNs certificate

1. On the menu sidebar, under SETTINGS, click Setup > Apple setup, and then click the APNs tab.
2. Click APNs certificate wizard.
3. On the Mode page, click Create a new APNs certificate.
4. On the CSR page, click Download certificate signing request.
   This saves the certificate signing request file apple.csr to your local computer.
5. You need an Apple ID. Even if you already have an ID, we recommend that you create a new one for use with Sophos Mobile. On the Apple ID page, click Create Apple ID in the Apple portal.
   This opens an Apple web page where you can create an Apple ID for your company.

   Note
   Store the credentials in a safe place where your colleagues can access them. Your company will need these credentials to renew the certificate each year.

6. In the wizard, enter your new Apple ID in the Apple ID field.
   This opens the Apple Push Certificates Portal.
8. Log in with your Apple ID and upload the certificate signing request file apple.csr.
9. Download the .pem APNs certificate file and save it to your computer.
10. On the Upload page, click Upload certificate and then browse for the .pem file that you received from the Apple Push Certificates Portal.
11. Click Save.

Sophos Mobile reads the certificate and displays the certificate details on the APNs tab.
7 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.

The EAS proxy is downloaded and installed separately from Sophos Mobile. It communicates with the Sophos Mobile server through an HTTPS web interface.

For a list of mail servers that the standalone EAS proxy supports, see the Sophos Mobile release notes.

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

Features

- 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 13).
- 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.
7.1 Download the EAS proxy installer

1. Sign in to Sophos Central Admin and go to Mobile.
2. On the menu sidebar, under SETTINGS, click Setup > Sophos 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.

7.2 Install the standalone EAS proxy

Prerequisites:

- 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.
- You know the URL of the Sophos Mobile server. See Determine the Sophos Mobile server URL (page 17).

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 Sophos Mobile server the EAS proxy will connect to.
   If required, select Use proxy server to configure a proxy server that the EAS proxy uses to connect to the Sophos Mobile server.
   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.
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.
   • 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)
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 iPhones and iPads 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.
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. Sign in to Sophos Central Admin and go to Mobile.

17. On the menu sidebar, under SETTINGS, click Setup > Sophos setup, and then click the EAS proxy tab.

18. Under External, click Upload a file. Upload the certificate created during configuration.

   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.

This completes the initial setup of the standalone EAS proxy.

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.
7.3 Set up email access control through PowerShell

When you set up the standalone EAS proxy in PowerShell mode, it connects to your Exchange mail server through PowerShell and sets email access based on the device’s compliance status.

In PowerShell mode, mail traffic goes directly from the Exchange mail server to your devices without a proxy. For a schematic of the communication flow, see the Sophos Mobile technical guide.

Advantages of the PowerShell mode:

- You do not need to open a port on your Sophos Mobile server for incoming email traffic from your devices.
- You can prevent devices that are not enrolled with Sophos Mobile from accessing email.

The Exchange mail server can be either Exchange Server or Exchange Online, which is part of Office 365. Supported versions are:

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

Restriction

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

To set up email access control through PowerShell, do as follows.

Related information

Sophos Mobile technical guide (Sophos Central)

Configure PowerShell

1. Optional: If required, install Windows PowerShell on the computer on which you are going to install the EAS proxy.
2. Open PowerShell as an administrator and run the following command:
   
   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   Exchange Server requires additional configuration:

3. Open the Exchange Management Shell.
4. Set the PowerShell execution policy:
   
   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. Get the name of the PowerShell virtual directory:
   
   ```
   Get-PowerShellVirtualDirectory -Server <server name>
   ```

   `<server name>` is the name of the computer on which Exchange Server is installed.

   In a standard installation, the PowerShell virtual directory is PowerShell (Default Web Site).
6. Set basic authentication for the PowerShell virtual directory:

   ```powershell
   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)" -BasicAuthentication $true
   ```

**Related information**

- Installing Windows PowerShell (Microsoft document)
- Open the Exchange Management Shell (Microsoft document)

---

**Create a service account**

A service account is a special user account on the Exchange mail server that Sophos Mobile uses to execute PowerShell commands.

1. Sign in to the relevant admin console:
   - For Exchange Server: Exchange Admin Center
   - For Exchange Online: Office 365 Admin Center

2. Create a user account.
   - Use a username 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.

3. 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 user account as a member.

---

**Configure the PowerShell connection**

1. Use the setup assistant as if you’re installing a standalone EAS proxy. On the EAS Proxy instance setup page, configure the following settings:

   - **Instance type**: Select PowerShell Exchange/Office 365.
   - **Instance name**: A name to identify the instance.
   - **Exchange server**: For Exchange Server, enter the name or IP address of your server.
     For Exchange Online, enter `outlook.office365.com` if you’re using the global Office 365 service. For other services, for example Office 365 Germany, you can find the address in the Microsoft document Connect to Exchange Online PowerShell.
     Don’t enter the protocol `https://` or the suffix `/powershell-liveid` to the name. The setup wizard adds these automatically.
   - **Allow all certificates**: The EAS proxy doesn’t verify the server certificate. Select this for example if you’re using Exchange Server with a self-signed certificate.
**Warning**
This setting reduces the security of mail server connections. Only select it if required by your network environment.

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

2. Click **Add** to add the instance to the **Instances** list.
3. Repeat the previous steps to set up PowerShell connections to other Exchange Server instances.
4. Complete the setup.
5. Optional: If required, configure a proxy server that the EAS proxy uses to connect to Exchange Server or Exchange Online. On the computer on which you’ve installed the EAS proxy, open a command prompt using the **Run as administrator** option and type the following command:

   ```bash
   netsh winhttp set proxy <server name or IP>:<port>
   ```

**Warning**
This command configures a system-wide proxy. Other programs running on the computer might be affected by this.

**Related information**
- Install the standalone EAS proxy (page 10)
- Connect to Exchange Online PowerShell (Microsoft document)

**Upload the PowerShell certificate**

Upload the certificate of the PowerShell connection to Sophos Mobile.

1. Sign in to Sophos Central Admin and go to **Mobile**.
2. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
3. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.
4. Under **External**, click **Upload a file**. Upload the certificate created during configuration.
   - If you have set up more than one instance, repeat this for all instance certificates.
5. Click **Save**.
6. In Windows, open the **Services** dialog and restart the **EASProxy** service.

**7.4 Block email access for unmanaged devices**

You can prevent devices that are not enrolled with Sophos Mobile from accessing email.

Prerequisite: You’ve set up the standalone EAS proxy in PowerShell mode.

In these instructions, Exchange refers to either your on-premise Exchange server or to your Exchange Online plan included in Office 365.
You can configure Exchange to quarantine unmanaged devices. Users will receive an email telling them to enroll the device with Sophos Mobile. After the device is enrolled, it’s automatically removed from quarantine.

**Warning**
Before you apply these settings in a production environment, ensure that your devices are enrolled and can synchronize with Sophos Mobile. All devices will be quarantined by default and will only have email access if the Sophos Mobile server sets them as compliant.

Also, enrolled devices are quarantined if the EAS proxy doesn’t know their compliance status. This might happen when a device hasn’t synchronized with Sophos Mobile for too long or when the EAS proxy can’t communicate with the Sophos Mobile server.

To block email access for unmanaged devices:

1. Open the Exchange Management Shell (if you have an Exchange server) or connect to Exchange Online PowerShell.
   For details, see the links in related information.
2. Run the following command (in one line):
   ```powershell
   Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine -UserMailInsert "Please enroll your device with Sophos Mobile."
   ```
   The text you specify with `-UserMailInsert` is added to the notification email that Exchange sends to users when their device is quarantined.

For more information on controlling email access in general, see the Microsoft document Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list.

**Related information**
- Set up the standalone EAS proxy in PowerShell mode (page 13)
- Open the Exchange Management Shell (Microsoft document)
- Connect to Exchange Online PowerShell (Microsoft document)
- Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list (Microsoft document)

### 7.5 Configure a connection to the standalone EAS proxy server

To configure the connection between Sophos Mobile and the standalone EAS proxy, you upload the certificate of the EAS proxy server to Sophos Mobile. The certificate was generated when you configured the EAS proxy instance.

For information on the installation and configuration of the standalone EAS proxy, see Standalone EAS proxy (page 9).
**Warning**
If the EAS proxy service is started before you have uploaded the certificate, Sophos Mobile rejects the connection to the server and the service fails to start.

To upload the certificate of the standalone EAS proxy:
1. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
2. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.
3. Under **External**, click **Upload a file** and navigate to the certificate file.
   - If you have set up more than one EAS proxy instance, repeat this for all instances.
4. Click **Save**.
5. In Windows, open the **Services** dialog and restart the **EASProxy** service.

### 7.6 Determine the Sophos Mobile server URL

You need the Sophos Mobile server URL to configure the standalone EAS proxy. The value is displayed in the Sophos Mobile system settings.

1. Sign in to Sophos Central Admin and go to **Mobile**.
2. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.

   Under **External**, the URL of the Sophos Mobile server is displayed.
8 Compliance policies

With compliance policies you can:

- Allow, forbid or enforce certain features of a device.
- Define actions that are executed when a compliance rule is violated.

You can create different compliance policies and assign them to device groups. This allows you to apply different levels of security to your managed devices.

Tip
If you are planning to manage both corporate and private devices, we recommend that you define separate compliance policies for at least these two device types.

8.1 Create compliance policy

1. On the menu sidebar, under CONFIGURE, click Compliance policies.
2. On the Compliance policies page, click Create compliance policy, and then select the template the policy will be based on:
   - Default template: A selection of compliance rules, with no actions defined.
   - PCI template, HIPAA template: Compliance rules and actions based on the HIPAA and the PCI DSS security standard, respectively.
   Your choice of template doesn’t restrict your subsequent configuration options.
3. Enter a name and, optionally, a description for the compliance policy. Repeat the following steps for all required platforms.
4. Make sure that the Enable platform check box on each tab is selected.
   If this check box is not selected, devices of that platform are not checked for compliance.
5. Under Rule, configure the compliance rules for the particular platform.
   For a description of the available rules for each device type, click Help in the page header.

Note
Each compliance rule has a fixed severity level (high, medium, low) that is depicted by a blue icon. The severity helps you to assess the importance of each rule and the actions you should implement when it is violated.

Note
For devices where Sophos Mobile manages the Sophos container instead of the whole device, only a subset of compliance rules is applicable. In Highlight rules, select a management type to highlight the rules that are relevant.

6. Under If rule is violated, define the actions that will be taken when a rule is violated:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny email</td>
<td>Forbid email access.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
|                 | This action can only be taken if you have configured a connection to the standalone EAS proxy. See Configure a connection to the standalone EAS proxy server (page 16).  
This action is only available for Android, iOS, Windows and Windows Mobile devices. |
| **Lock container** | Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps.  
This action can only be taken when you have activated a Mobile Advanced license.  
This action is only available for Android devices, iPhones, and iPads. |
| **Set health**  | Select the health status **(Red, Yellow, Green)** the device gets if it violates this rule. If the device violates more than one rule, it gets its health status from the rule that's associated with the worst health.  
Sophos Mobile reports the health status to Sophos Wireless. Depending on your Sophos Wireless configuration, network access is restricted.  
This action is available for Android devices, iPhones, and iPads if you've turned on Synchronized Security. |
| **Create alert** | Trigger an alert.  
The alerts are displayed on the **Alerts** page of Sophos Central Admin. |
| **Transfer task bundle** | Transfer a specific task bundle to the device.  
We recommend that you set this to **None** at this stage. For further information, see the Sophos Mobile administrator help.  
**CAUTION**  
When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required. |

**Note**  
When an Android Enterprise fully managed device becomes non-compliant, all apps are disabled.

7. When you have made the settings for all required platforms, click **Save** to save the compliance policy under the name that you specified.  
To make use of a compliance policy, you assign it to a device group. This is described in the next section.
9 Device groups

Device groups are used to categorize devices. They help you to manage devices efficiently as you can carry out tasks on a group rather than on individual devices.

A device always belongs to exactly one device group. You assign a device to a device group when you add it to Sophos Mobile.

Tip
Only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

9.1 Create device group

1. On the menu sidebar, under MANAGE, click Device groups, and then click Create device group.
2. On the Edit device group page, enter a name and a description for the new device group.
3. Under Compliance policies, select the compliance policies that are applied to corporate and to personal devices.
4. Click Save.

Note
The device group settings contain the Enable iOS auto-enrollment option. This option allows you to enroll iPhones and iPads with Apple Configurator. For further information, see the Sophos Mobile administrator help.

The new device group is created and shown on the Device groups page.
10 Get started with device policies

The Policies startup wizard helps you create basic device policies for all platforms. You can enhance the policies later.

**Restriction**
These instructions don’t apply to Chrome devices.

To create policies with the Policies startup wizard:
1. On the dashboard, click Policies startup wizard in the Getting started tasks widget.
   
   Tip
   If you don’t see the widget, click Add widget > Getting started.

2. On the Platforms page, select the device platforms for which you want to create a policy.
   Select Android and iOS & iPadOS.
3. For Android, you can select a management mode.
   This setting affects which policy types are available. We recommend you use the Android Enterprise mode.
4. On the Policies page, configure the following settings:
   a) Enter a name for the policy.
      For each platform, a policy with this name is created.
   b) Select the areas the policy manages.
      If you clear a check box, the corresponding wizard page is skipped. You can configure the skipped areas (and more) later.
      We suggest you select at least Password requirements and Restrictions.
5. On the Passwords page, configure requirements for the device password.
6. On the Restrictions page, configure restrictions applied to devices, like turning off the camera or other device features that could be a security risk.
7. On the Wi-Fi page, configure the connection to your corporate Wi-Fi network.
   If your Wi-Fi network uses a different security type than WPA/WPA2 PSK, you can change that setting later.
8. On the Email page, configure the connection to your corporate Microsoft Exchange email server.
   The placeholders %_USERNAME_% and %_EMAILADDRESS_% are replaced by the name and the email address of the user assigned to the device.
9. Click Finish.

For each platform you’ve selected, the wizard creates a policy.

To view the policy, click Policies in the menu sidebar and then click the device platform.

To change the areas managed, click the policy’s name and then click Add configuration.

You must set up Android Enterprise for your organization before you can enroll devices. See the Sophos Mobile administrator help.
11 Create task bundle for Android devices

You create separate task bundles for Android, iOS, and other device platforms you want to manage. To create an enrollment task bundle for your Android devices:

1. On the menu sidebar, under CONFIGURE, select Task bundles > Android.
2. On the Task bundles page, select Create task bundle.
3. On the Edit task bundle page, enter a name and, optionally, a description for the task bundle.
   The version is automatically incremented every time you save the task bundle.
4. Optional: If you select Selectable for compliance actions, you can transfer the task bundle to devices when they become non-compliant.
   You configure this in a compliance policy.
5. Select Add task > Enroll. You’re guided through adding an enrollment task to the task bundle.
   a) Optional: Change the name of the task.
      The name will be displayed in the Self Service Portal when the device is enrolled.
   b) Select the enrollment type.
      To enroll Android Enterprise fully managed devices with this task bundle, select Full device.
   c) On the next page, select the policy that will be assigned to the device when it’s enrolled.
      Only policies that match the enrollment type you’ve selected are displayed.
   d) Select Finish.
6. Optional: Select Add task > Assign policy to add more policies to the task bundle, for example if you’ve configured separate policies for Exchange, VPN, or Wi-Fi settings.
7. Optional: Add more tasks to the task bundle, for example to install apps or to display a message on the device.
8. Optional: Change the installation order of the tasks by using the arrow icons on the right-hand side of the tasks list.
12 Create task bundle for iPhones and iPads

You create separate task bundles for Android, iOS, and other device platforms you want to manage.

To create an enrollment task bundle for your iPhones and iPads:

1. On the menu sidebar, under **CONFIGURE**, select **Task bundles > iOS & iPadOS**.
2. On the **Task bundles** page, select **Create task bundle**.
3. On the **Edit task bundle** page, enter a name and, optionally, a description for the task bundle. The version is automatically incremented every time you save the task bundle.
4. Optional: If you select **Selectable for compliance actions**, you can transfer the task bundle to devices when they become non-compliant. You configure this in a compliance policy.
5. Optional: Select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails. This option is only available if the task bundle contains an **Install app** task.
6. Select **Add task > Enroll**. You’re guided through adding an enrollment task to the task bundle.
   a) Optional: Change the name of the task. The name will be displayed in the Self Service Portal when the device is enrolled.
   b) Select the enrollment type. To enroll fully managed devices with this task bundle, select **Full MDM**.
   c) On the next page, select the policy that will be assigned to the device when it’s enrolled. Only policies that match the enrollment type you’ve selected are displayed.
   d) Select **Finish**.
7. Optional: Select **Add task > Assign policy** to add more policies to the task bundle, for example if you’ve configured separate policies for Exchange, VPN, or Wi-Fi settings.
8. Optional: Add more tasks to the task bundle, for example to install apps or to display a message on the device.
9. Optional: Change the installation order of the tasks by using the arrow icons on the right-hand side of the tasks list.
13 Create Self Service Portal configurations

With a Self Service Portal configuration, you configure the types of devices that users can enroll, the enrollment details, and the device actions they can perform in the Self Service Portal.

You can use different Self Service Portal configurations for different users. To do so, add users to a user group and associate the group with a configuration. You can find details on user groups in related information.

If a user belongs to several groups that are all associated with Self Service Portal configurations, the configuration with the highest priority applies.

To create a Self Service Portal configuration:

1. On the menu sidebar, under SETTINGs, select Setup > Self Service Portal.
2. Select Enrollment texts and then add a terms of use text and a post-enrollment text. When you assign these texts to your Self Service Portal configuration, they are displayed before and after the enrollment, respectively.
3. On the Self Service Portal configurations page, select Add to create a configuration.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the configuration. In the Self Service Portal, users select a configuration by this name.</td>
</tr>
<tr>
<td>User groups</td>
<td>Select Add and then enter a user group. The configuration is applied to all members of that group.</td>
</tr>
<tr>
<td>Maximum number of devices</td>
<td>The maximum number of devices a user can enroll in the Self Service Portal.</td>
</tr>
<tr>
<td>Actions</td>
<td>Select Show and then select the management actions a user can perform in the Self Service Portal.</td>
</tr>
</tbody>
</table>

5. Select Add > Android.
6. In the Configure platform settings dialog, configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>The name of the platform settings. In the Self Service Portal, users select an enrollment type by this name.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the platform settings. This description is displayed in the Self Service Portal next to the name.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>The owner mode (corporate or personal) of devices enrolled with this configuration.</td>
</tr>
<tr>
<td><strong>Device group</strong></td>
<td>The device group the device is added to.</td>
</tr>
<tr>
<td><strong>Enrollment package</strong></td>
<td>Select the Android task bundle you’ve created.</td>
</tr>
<tr>
<td><strong>Terms of use</strong></td>
<td>The text to be displayed in the Self Service Portal before the enrollment. Leave this field empty to display no text. Users must agree to the text to proceed with the enrollment.</td>
</tr>
<tr>
<td><strong>Post-enrollment text</strong></td>
<td>The text to be displayed in the Self Service Portal after the enrollment. Leave this field empty to display no text.</td>
</tr>
</tbody>
</table>

7. Select **Apply** to add the platform settings to the Self Service Portal configuration.
8. Select **Add > iOS & iPadOS**, and then repeat the configuration steps you performed for Android.
9. On the **Edit Self Service Portal configuration** page, select **Save**.

There always is a **Default** configuration. This configuration has the lowest priority, so that it is only used when no other configuration matches a user.
14 Test device enrollment through the Self Service Portal

We recommend that you test device enrollment through the Self Service Portal before you roll out the Self Service Portal to your users.

Log in to the Self Service Portal with a test user account you created for yourself and perform test enrollments for all platforms that you want to manage with Sophos Mobile.
15 Use the **Add device** wizard

You can easily enroll new devices with the **Add device** wizard. It provides a workflow that combines the following tasks:

- Add a new device to Sophos Mobile.
- Optional: Assign a user to the device.
- Enroll the device.
- Optional: Transfer a task bundle to the device.

1. On the menu sidebar, under **MANAGE**, click **Devices**, and then click **Add > Add device wizard**.

   **Tip**
   
   Alternatively, you can start the wizard in the following ways:
   
   - From the **Dashboard** page by clicking the **Add device** widget.
   - From the Sophos Central Admin menu by clicking **Protect Devices > Start device enrollment wizard**.

2. On the **User** page, either enter search criteria to look up a user the device will be assigned to, or select **Skip user assignment** to enroll a device that will not be assigned to a user yet.

   **Note**
   
   You can search for partial strings, but only from the start of a field. For example, the search string `example` matches `Example User` and `example@company.com` but not `user@example.com`.

3. On the **User selection** page, select the required user from the list of users matching your search criteria.

4. On the **Device details** page, configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>The device platform.</td>
</tr>
<tr>
<td>Name</td>
<td>A unique name under which the device will be managed by Sophos Mobile.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the device.</td>
</tr>
<tr>
<td>Phone number</td>
<td>An optional phone number. Enter the number in international format, for example <code>+491701234567</code>.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address to which the enrollment instructions are sent. This is the email address of the user assigned to the device, as configured in Sophos Central user management.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select the device owner type: either <strong>Corporate</strong> or <strong>Personal</strong>.</td>
</tr>
<tr>
<td>Device group</td>
<td>Select the device group the device will be assigned to. If you have not created a device group yet, you can select the device group <strong>Default</strong>, which is always available.</td>
</tr>
</tbody>
</table>
5. On the **Enrollment type** page, select whether you want to enroll the device or only the Sophos container.

   Select **Enroll device**.

6. Select the task bundle you’ve configured for the device platform.

7. On the **Enrollment** page, follow the instructions to complete the enrollment process.

8. When enrollment has been completed successfully, click **Finish**.

**Note**

- When you have made all the selections, you can close the wizard without having to wait for the **Finish** button to appear. An enrollment task is created and processed in the background.
16 Glossary

**ad hoc provisioning profile**
A distribution provisioning profile you add to a self-developed iOS app. This allows you to install the app on designated devices without having to publish it to the App Store.

**enrollment**
The registration of a device with Sophos Mobile.

**Enterprise App Store**
An app repository that is hosted on the Sophos Mobile server. The administrator can use Sophos Mobile Admin to add apps to the Enterprise App Store. Users can then use the Sophos Mobile Control app to install these apps onto their devices.

**Mobile Advanced license**
With a license of type Mobile Advanced you can manage Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.

**provisioning**
The process of installing the Sophos Mobile Control app on a device.

**Sophos Central Admin**
The web interface that you use to manage devices.

**Sophos Central Self Service portal**
The web interface that allows users to enroll their own devices and carry out other tasks without having to contact the helpdesk.

**Sophos Mobile client**
The Sophos Mobile Control app that is installed onto devices managed by Sophos Mobile.

**Sophos Intercept X for Mobile**
A security app for Android devices, iPhones, and iPads. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.

**Sophos Secure Email**
An app for Android devices, iPhones, and iPads that provides a secure container for managing your email, calendar and contacts. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.

**Sophos Secure Workspace**
An app for Android devices, iPhones, and iPads that provides a secure workspace where you can browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.

**task bundle**
You create a package to bundle several tasks into one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.
Team ID

Every iOS and macOS app is signed by a Team ID. The Team ID is supplied by Apple and is unique to a specific development team.
17 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.


• Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
18 Legal notices

Copyright © 2020 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.