

**SOPHOS**

Security made simple.

# Sophos Mobile

## startup guide

Product Version: 8.1



# Contents

About this guide.....	1
Sophos Mobile licenses.....	2
Trial licenses.....	2
Upgrade trial licenses to full licenses.....	2
Update licenses.....	2
What are the key steps?.....	3
Log in as super administrator.....	4
Run the configuration wizard.....	5
Activate Mobile Advanced licenses.....	7
Check your licenses.....	8
Create a customer.....	9
Switch to the customer.....	11
Create an administrator for the customer.....	12
Configure settings.....	13
Configure personal settings.....	13
Configure password policies.....	14
Configure technical support contact details.....	14
Configure Self Service Portal settings.....	15
Apple Push Notification service certificates.....	16
Requirements.....	16
Create an APNs certificate.....	16
Compliance policies.....	18
Create compliance policy.....	18
Device groups.....	20
Create device group.....	20
Configure iOS devices.....	21
Create iOS device profile.....	21
Create task bundle for iOS devices.....	22
Configure Android devices.....	23
Create Android device profile.....	23
Create task bundle for Android devices.....	24
Update Self Service Portal settings.....	25
Create a Self Service Portal test user.....	26
Test device enrollment through the Self Service Portal.....	27
Import users into Sophos Mobile.....	28
Use the device enrollment wizard to assign and enroll new devices.....	29
Glossary.....	31
Technical support.....	32
Legal notices.....	33

# 1 About this guide

This guide explains how to set up Sophos Mobile step by step to manage your devices.

Further information is available in the [Sophos Mobile administrator help](#).

This guide focuses on Android and iOS as the most common mobile platforms. The settings apply to the other supported operating systems in a similar way.

## 2 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.

For further information on managing Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email with Sophos Mobile, see the [Sophos Mobile administrator help](#).

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.

### 2.1 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.

### 2.2 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](#).

### 2.3 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](#).

## 3 What are the key steps?

To start using Sophos Mobile:

1. Log in to Sophos Mobile Admin as a super administrator.
2. Start the configuration wizard to carry out initial configuration of the Sophos Mobile server.

### Note

The configuration wizard includes an option to request a trial license.

3. Check your licenses.
4. Create a new customer for managing your devices.
5. Switch to the new customer.
6. Create an administrator for the new customer and log in to Sophos Mobile Admin as that administrator.
7. Configure personal settings, password policies for administrator accounts, technical support contact details, and settings for the Self Service Portal.
8. Upload an Apple Push Notification service certificate to manage iOS devices.
9. Create compliance policies.
10. Create device groups.
11. Configure devices.
12. Update Self Service Portal settings and add a Self Service Portal test user.
13. If you use internal user management: Add users either by creating them or by uploading your user list.
14. If you use external user management: Configure the connection to your LDAP directory.  
This is described in the *Sophos Mobile super administrator guide*.
15. Test device enrollment in the Self Service Portal.

## 4 Log in as super administrator

You must log in to Sophos Mobile Admin using the super administrator account that was configured during the installation of Sophos Mobile to perform some initial configuration steps.

1. Open the Sophos Mobile Admin web address that you configured during installation of Sophos Mobile.
2. In the login dialog, enter the super administrator customer name and the credentials of the super administrator, then click **Login**.

### Note

When you log in as a super administrator, you get a special version of Sophos Mobile Admin adapted to super administrator tasks.

For a detailed description of how to use Sophos Mobile Admin as a super administrator, see the *Sophos Mobile super administrator guide*.

## 5 Run the configuration wizard

When you log in to Sophos Mobile Admin for the first time after installation, a configuration wizard is started to configure certain server settings.

You need to provide:

- A Mobile Standard license key, optionally an additional Mobile Advanced license key
- SSL/TLS certificate(s)
- SMTP credentials

### Note

As a super administrator you can adjust these settings afterward on the **System setup** page of Sophos Mobile Admin. To open the **System setup** page from the menu sidebar, click **SETTINGS > Setup > System setup**.

To run the configuration wizard:

1. After you have logged in to Sophos Mobile Admin for the first time as super administrator, the **Welcome** view is displayed. Click **Next**.
2. In the **License** view, enter your Mobile Standard license key or request a trial license:
  - Mobile Standard license key:
 

When you enter the Mobile Standard license key and click **Activate**, you are given the option to additionally enter a Mobile Advanced license key. If you have purchased Mobile Advanced licenses, enter the key in **Advanced license key**.
  - Request a trial license:
 

To request a trial license click **Request trial** and enter the email address you used when you registered to download the Sophos Mobile installer from [www.sophos.com](http://www.sophos.com). Then click **Request trial** again.

### Note

You can change the license settings at any time in Sophos Mobile Admin.

Click **Next**.

3. In the **SSL/TLS** view, configure the certificates to be used for securing the SSL or TLS connection between the Sophos Mobile server and the clients.
 

You can configure up to four certificates because, depending on your network architecture, different certificates for clients connecting from the Internet or from your local intranet may be in use. The Sophos Mobile server will communicate the list of certificates to the clients. On establishing an SSL or TLS connection, the clients will only trust the server if the presented certificate is included in the list (*certificate pinning*).

  - a) Click **Auto-discover certificate(s)**.
 

In most cases the auto-discover function is sufficient to discover the certificates currently in use.
  - b) If the certificates cannot be discovered automatically, you can upload them manually by clicking **Upload a file** and selecting the relevant CER or DER file.
 

The certificates are displayed in the **SSL/TLS** view.

**Important**

Update the list when you have changed or renewed SSL certificates. At any given time, at least one valid certificate must be available. Otherwise the clients will not trust the server and will not connect to it.

4. In the **SMTP** view, configure the SMTP server information and logon credentials. SMTP must be configured to enable emails to be sent to new users, providing them with logon credentials. It also needs to be configured to enable enrollment through email.

Option	Description
<b>SMTP host</b>	The SMTP server address.
<b>Connection port</b>	<p>The server port to connect to.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b> The displayed connection types (TLS, SSL, and unencrypted) only show standard port usages. See the documentation of the SMTP server for guidelines on which port to use.</p> </div>
<b>SMTP user</b>	If required by the SMTP server, enter the name of a user that is allowed to connect.
<b>SMTP password</b>	The password of the SMTP user.
<b>Email originator</b>	The email address that will appear in the <i>From</i> field of emails from Sophos Mobile.
<b>Originator name</b>	<p>The author name that will appear in the <i>From</i> field.</p> <p>If required, you can configure a different originator name (but not email address) for each customer later on. See the <a href="#">Sophos Mobile administrator help</a>.</p>
<b>Send error emails</b>	Sophos Mobile will send error emails, for example when an APNs certificate expires.
<b>Email recipients</b>	Enter email addresses of the recipients that will receive error emails.

**Note**

Sophos Mobile does not support the OAUTH mechanism for SMTP authentication. Email providers that prefer OAUTH (like for example Google Gmail) might classify sign-in attempts from Sophos Mobile as insecure.

5. After you have configured the relevant information, click **Send test email** to verify the email configuration.
6. Click **Save**.



## 6 Activate Mobile Advanced licenses

With Mobile Advanced licenses you can use Sophos Mobile to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.

If Mobile Advanced licenses have not been activated during the initial configuration of Sophos Mobile, the super administrator can activate them later from Sophos Mobile Admin:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **License** tab, enter your license key in **Advanced license key** and click **Activate**.

When the key is activated, the license details are displayed.

## 7 Check your licenses

Sophos Mobile uses a user-based license scheme. One user license is valid for all devices assigned to that user. Devices that are not assigned to a user require one license each.

To check your available licenses:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **System setup** page, click the **License** tab.

The following information is displayed:

- **Maximum number of licenses:** Maximum number of device users (and unassigned devices) that can be managed.  
If the super administrator did not set a quota for the customer, the number of licenses is limited by the overall number for the Sophos Mobile server.
- **Used licenses:** Number of licenses in use.
- **Valid until:** The license expiration date.
- **Licensed URL:** The URL of the Sophos Mobile server for which the license is issued.

If you have any questions or concerns regarding the displayed license information, contact your Sophos sales representative.

## 8 Create a customer

You must be logged in to Sophos Mobile Admin as a super administrator to perform this task.

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. Click **Create customer**.
3. On the **Edit customer** page, configure the following settings.

Option	Description
<b>Name</b>	The customer's name.
<b>Description</b>	Text to describe the purpose of the customer account.
<b>Maximum number of licenses</b>	The number of device users and unassigned devices that can be managed for the customer.
<b>Advanced licenses</b>	If selected, the customer can use Sophos Mobile to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.
<b>Valid until</b>	The expiration date for the licenses that are assigned to the customer. After that date, you cannot create new tasks for devices that are managed for the customer.
<b>Deactivate account</b>	If selected, logging in to that customer is disabled. As super administrator, you can still switch to the customer's view, using the customer list in the page header.  A deactivated account can be activated again by deselecting the <b>Deactivate account</b> check box.
<b>Activated platforms</b>	Select the platforms for which devices can be enrolled.
<b>Locate devices</b>	Select <b>Allowed for users</b> to enable users to locate their devices if they are lost or stolen. Select <b>Allowed for administrators</b> to enable administrators to locate devices.
<b>Clone settings</b>	Select the <b>Settings and packages</b> check box if you want all profiles, bundles, and packages created in the super administrator account to be available in the customer's account.
<b>User directory</b>	Select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile.  Choose from: <ul style="list-style-type: none"> <li>• <b>None. No SSP, user-specific profiles, or LDAP administrators available:</b> This disables the creation of user accounts for the Self Service Portal, and the lookup of accounts for Sophos Mobile Admin from an LDAP directory.</li> <li>• <b>Internal directory:</b> Use internal user management for Sophos Mobile Admin and the Self Service Portal. For further information, see the <a href="#">Sophos Mobile administrator help</a>.</li> <li>• <b>External LDAP directory:</b> In addition to internal user management, you can lookup accounts for Sophos Mobile</li> </ul>

Option	Description
	Admin and the Self Service Portal from an LDAP directory. Click <b>Configure external LDAP</b> to specify the server details.

4. Click **Save**.

The customer is created.

## 9 Switch to the customer

To complete the initial configuration of the customer that you created in the previous section, you need to switch from the super administrator customer to that customer.

To switch to the view of the new customer:

1. In the page header of the super administrator view, click the current customer name to open the list of available customers.

In that list, the super administrator customer is marked by an asterisk and shown at the top.

2. Select the customer you created in the previous section.

The view changes to the view of that customer, that is the view that you get when you log in with an administrator account for that customer.

## 10 Create an administrator for the customer

1. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators**.
2. On the **Show administrators** page, click **Create administrator**.
3. On the **Edit administrator** page, configure the account details for the administrator.
  - When **External LDAP directory** is selected as the user directory for the customer, you can click **Lookup user via LDAP** to select an existing LDAP account.
  - When **Internal directory** or **None** is selected as user directory for the customer, enter the relevant data in the **Login name**, **First name**, **Last name**, **Email address** and **Password** fields.

The password that you specify is a one-time password. At first login, the administrator will be prompted to change it.

4. In the **Role** list, select the **Administrator** user role.
5. Click **Save** to create the administrator account.

To proceed with the configuration of the customer, log out from Sophos Mobile Admin and log in again, using the credentials of the administrator that you just created (customer name, login name, one-time password).

# 11 Configure settings

Configure the following settings:

- Personal settings, for example the platforms you want to manage
- Password policies
- Technical support contact details
- Self Service Portal settings

## 11.1 Configure personal settings

To use Sophos Mobile Admin more efficiently, you can customize the user interface to show only the platforms you work with.

### Note

By configuring the platforms you only change the view of the user who is currently logged in. You cannot deactivate any functions here.

Prerequisite: You have logged in to Sophos Mobile Admin as the administrator you have created for the new customer.

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

Option	Description
Language	Select the language for Sophos Mobile Admin.
Timezone	Select the timezone in which dates are shown.
Unit system	Select the unit system for length values ( <b>Metric</b> or <b>Imperial</b> ).
Lines per page in tables	Select the maximum number of table lines you want to display per page.
Show extended device details	Select this check box to show all available information about the device. The <b>Custom properties</b> and <b>Internal properties</b> tabs will be added to the <b>Show device</b> page.
Activated platforms	<p>Select the platforms you want to manage for the customer:</p> <ul style="list-style-type: none"> <li>• <b>Android</b></li> <li>• <b>Android Things</b></li> <li>• <b>iOS</b></li> <li>• <b>Windows Mobile</b> (includes Windows Phone 8.1 and Windows 10 Mobile operating systems)</li> <li>• <b>Windows</b></li> <li>• <b>Windows IoT</b></li> </ul> <p>Based on your platform selection, the Sophos Mobile Admin user interface is adjusted. Only views and features that are relevant for the selected platforms are shown.</p>

Option	Description
	<p><b>Note</b></p> <p>The list of available platforms depends on your platform settings from the super administrator configuration. For further information, see the <a href="#">Sophos Mobile super administrator guide</a>.</p>

3. Click **Save**.

## 11.2 Configure password policies

To enforce password security, configure password policies for Sophos Mobile Admin users and the Self Service Portal.

### Note

The password policies do not apply to users from an external LDAP directory. For information on external user management, see the [Sophos Mobile super administrator guide](#).

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Password policies** tab.
2. Under **Rules**, you can define password requirements, like a minimum number of lower-case, upper-case or numerical characters that a password must contain to be valid.
3. Under **Settings**, configure the following settings:
  - a) **Password change interval (days)**: Enter the number of days until a password expires (between 1 and 730), or leave the field empty to disable password expiration.
  - b) **Number of previous passwords which must not be reused**: Select a value between 1 and 10, or select --- to disable this restriction.
  - c) **Maximum number of failed login attempts**: Select the number of failed login attempts until the account gets locked (between 1 and 10), or select --- to allow an unlimited number of failed login attempts.
4. Click **Save**.

## 11.3 Configure technical support contact details

To support users who have questions or problems, you can provide them with details of how to contact technical support. The information that you enter here is displayed in the Sophos Mobile Control app and in the Self Service Portal.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Technical contact** tab.
2. Enter the required information for the technical contact.
3. Click **Save**.



## 11.4 Configure Self Service Portal settings

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**.  
The **Self Service Portal** page opens.
2. On the **Configuration** tab, configure the Self Service Portal settings as required.  
If you are not sure which settings to apply at this stage, we recommend that you use the default settings.  
For a detailed description of the settings, click **Help** in the page header.
3. On the **Terms of use** tab, click **Edit** to enter a mobile policy, disclaimer or agreement text.  
This text is displayed at the beginning of the device registration. Users have to accept the text before they can perform the registration.

### Tip

You can use the editor toolbar to apply basic HTML formatting to the text. This also applies to the post-install text described in the next step.

4. Optional: On the **Post-install text** tab, click **Edit** to enter text that is displayed at the end of the device registration.  
You can use this text to explain any steps the user has to perform after the registration.
5. Click **Save**.

## 12 Apple Push Notification service certificates

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

Sophos Mobile manages APNs certificates per customer. You must create and upload the certificates for each customer that you use.

APNs certificates have a validity period of one year.

To facilitate the renewal of APNs certificates, the super administrator can in one step renew the certificates of all customers that use the same certificate. See the [Sophos Mobile administrator help](#).

The following sections describe the requirements that must be fulfilled and the steps you must take to get access to the APNs servers with your own client certificate.

### 12.1 Requirements

For communication with the Apple Push Notification Service (APNs), TCP traffic to and from the following ports must be allowed:

- The Sophos Mobile server needs to connect to `gateway.push.apple.com:2195 TCP (17.0.0.0/8)`
- Each iOS device with Wi-Fi only access needs to connect to `*.push.apple.com:5223 TCP (17.0.0.0/8)`

### 12.2 Create an APNs certificate

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **APNs** tab. The description on that tab guides you through the steps you have to perform to request a certificate from Apple and to upload it to Sophos Mobile.
2. In the **Download certificate signing request** step, click **Download certificate signing request**. This saves the certificate signing request file `apple.csr` to your local computer. The signing request file is specific to the current customer.
3. 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. In the **Create Apple ID** step, click **Create a new Apple ID**. 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.

4. For your reference, enter your new Apple ID in the **Apple ID** field on the top of the **APNs** tab. When you renew the certificate each year, you must always use that same Apple ID.
5. In the **Create or renew APNs certificate** step, click **Apple Push Certificates Portal**.

This opens the Apple Push Certificates Portal.

6. Log in with your Apple ID and upload the certificate signing request file `apple.csr`.
7. Download the `.pem` APNs certificate file and save it to your computer.
8. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.
9. Click **Save** to add the APNs certificate to Sophos Mobile.

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

# 13 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.

## 13.1 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:

Option	Description
<b>Deny email</b>	<p>Forbid email access.</p> <p>This action can only be taken if the super administrator has configured a connection to the internal or to the standalone EAS proxy. See the <a href="#">Sophos Mobile super administrator guide</a>.</p> <p>This action is only available for Android, iOS, Windows and Windows Mobile devices.</p>
<b>Lock container</b>	<p>Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps.</p> <p>This action can only be taken when you have activated a Mobile Advanced license.</p> <p>This action is only available for Android and iOS devices.</p>
<b>Deny network</b>	<p>Forbid network access.</p> <p>This action can only be taken if the super administrator has configured Network Access Control. See the <a href="#">Sophos Mobile super administrator guide</a>.</p>
<b>Create alert</b>	<p>Create an alert.</p> <p>The alerts are displayed on the <b>Alerts</b> page.</p>
<b>Transfer task bundle</b>	<p>Transfer a specific task bundle to the device.</p> <p>This action is only available for Android, iOS, macOS and Windows devices.</p> <p>We recommend that you set this to <b>None</b> at this stage. For further information, see the <a href="#">Sophos Mobile administrator help</a>.</p> <div data-bbox="671 1221 1439 1449" style="background-color: #f0f0f0; padding: 10px;"> <p><b>Important</b></p> <p>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.</p> </div>

- When you have made the settings for all required platforms, click **Save** to save the compliance policy under the name that you specified.  
The new compliance policy is displayed on the **Compliance policies** page.

To make use of a compliance policy, you assign it to a device group. This is described in the next section.

# 14 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.

## 14.1 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 iOS devices with the Apple Configurator. For further information, see the [Sophos Mobile administrator help](#).

The new device group is created and shown on the **Device groups** page.

# 15 Configure iOS devices

## 15.1 Create iOS device profile

In this step, you create a profile for initial configuration of iOS devices.

We recommend that you set up separate profiles for:

- Password policies and restrictions
- Exchange account settings (if required)
- VPN settings (if required)
- Wi-Fi settings (if required)
- Root and client certificates (if required)

### Note

Sophos Mobile offers two methods for creating profiles for iOS devices:

- Create profiles directly in Sophos Mobile Admin.
- Import profiles created with Apple Configurator.

This section describes how to create profiles in Sophos Mobile Admin. For information on how to import profiles created with Apple Configurator, see the [Sophos Mobile administrator help](#).

To create an iOS device profile for password policies and restrictions:

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > iOS**.
2. On the **Profiles and policies** page, click **Create > Device profile**.
3. On the **Edit profile** page, configure the following settings:
  - a) **Name:** Enter a name for the profile. We recommend that you use the name `iOS SSP profile` for profiles that are applied during enrollment in the Self Service Portal.
  - b) **Organisation:** Enter the name of the organization for the profile, for example a company name.
  - c) **Description:** Enter a description for the profile, for example `base profile`.
4. To add password policies to the profile, click **Add configuration** and then select **Password policies**.
5. On the **Password policies** page, configure the required password settings.  
For a detailed description of the settings, click **Help** in the page header.
6. Click **Apply** to save your settings.  
The **Password policies** configuration is displayed on the **Edit profile** page under **Configurations**.
7. To add restrictions to the profile, click **Add configuration** again and then select **Restrictions**.
8. On the **Restrictions** page, select the required restrictions.

Some restrictions require a certain device type or iOS version. These requirements are shown to the right of each restriction.

For a detailed description of the settings, click **Help** in the page header.

9. Click **Apply** to save your settings.  
The **Restrictions** configuration is displayed on the **Edit profile** page under **Configurations**.
10. On the **Edit profile** page, click **Save** to save the profile.

The profile is displayed on the **Profiles and policies** page and is available for transfer onto iOS devices.

If required, create additional profiles for Exchange account settings, VPN settings, Wi-Fi settings and for the installation of root and client certificates.

## 15.2 Create task bundle for iOS devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles > iOS**.
2. On the **Task bundles** page, click **Create task bundle**.  
The **Edit task bundle** page is displayed.
3. Enter a name and, optionally, a description for the new task bundle in the relevant fields.  
The version is automatically incremented every time you save the task bundle.
4. Optional: Select **Selectable for compliance actions** to transfer the task bundle onto a device when it violates a compliance rule. See [Compliance policies](#) (page 18).

### Note

This option is disabled when you edit an existing task bundle and the task bundle is already used as a compliance action.

5. Optional: For iOS task bundles, select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails.  
This option is disabled when the task bundle contains no **Install app** task.
6. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task.  
The name that you enter here will be displayed in the Self Service Portal while the task is processed.
7. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example `Install password policies profile`, and select the profile you have created. Click **Apply** to create the task.
8. If you have configured profiles for Exchange, VPN or Wi-Fi settings, repeat the previous step for each profile.
9. Optional: Add further tasks to the task bundle.

### Tip

You can change the installation order of the tasks by using the sort arrows on the right-hand side of the tasks list.

10. After you have added all required tasks to the task bundle, click **Save** on the **Edit task bundle** page.

The task bundle is available for transfer. It is displayed on the **Task bundles** page.



# 16 Configure Android devices

## 16.1 Create Android device profile

In this step, you create a profile for initial configuration of Android devices.

We recommend that you set up separate profiles for:

- Password policies and restrictions
- Exchange account settings (if required)
- VPN settings (if required)
- Wi-Fi settings (if required)
- Root and client certificates (if required)

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > Android**.
2. On the **Profiles and policies** page, click **Create > Device profile**.
3. On the **Edit profile** page, configure the following settings:
  - a) **Name**: Enter a name for the profile. We recommend that you use the name `Android SSP profile` for profiles that are applied during enrollment in the Self Service Portal.
  - b) Optional: **Description**: Enter a description for the profile, for example `base profile`.
4. To add password policies to the profile, click **Add configuration** and then select **Password policies**.  
The **Password policies** page opens.
5. In the **Password type** field, select the type of password you want to define, for example **Complex**.
6. Configure the required password settings.  
The available settings depend on the password type that you selected. For a detailed description of all settings, click **Help** in the page header.
7. Click **Apply** to save your settings.  
The **Password policies** configuration is displayed on the **Edit profile** page under **Configurations**.
8. To add restrictions to the profile, click **Add configuration** again and then select **Restrictions**.
9. On the **Restrictions** page, select the required restrictions.  
  
Some restrictions require a certain device type or Android version. These requirements are shown to the right of each restriction.  
  
For a detailed description of the settings, click **Help** in the page header.
10. Click **Apply** to save your settings.  
The **Restrictions** configuration is displayed on the **Edit profile** page under **Configurations**.
11. On the **Edit profile** page, click **Save** to save the profile.

The profile is displayed on the **Profiles and policies** page and is available for transfer onto Android devices.

If required, create additional profiles for Exchange account settings, VPN settings, Wi-Fi settings and for the installation of root and client certificates.

## 16.2 Create task bundle for Android devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles > Android**.
2. On the **Task bundles** page, click **Create task bundle**.  
The **Edit task bundle** page is displayed.
3. Enter a name and, optionally, a description for the new task bundle in the relevant fields.  
The version is automatically incremented every time you save the task bundle.
4. Optional: Select **Selectable for compliance actions** to transfer the task bundle onto a device when it violates a compliance rule. See [Compliance policies](#) (page 18).

### Note

This option is disabled when you edit an existing task bundle and the task bundle is already used as a compliance action.

5. Optional: For iOS task bundles, select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails.  
This option is disabled when the task bundle contains no **Install app** task.
6. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task.  
The name that you enter here will be displayed in the Self Service Portal while the task is processed.
7. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example `Install password policies profile`, and select the profile you have created. Click **Apply** to create the task.
8. If you have configured profiles for Exchange, VPN or Wi-Fi settings, repeat the previous step for each profile.
9. Optional: Add further tasks to the task bundle.

### Tip

You can change the installation order of the tasks by using the sort arrows on the right-hand side of the tasks list.

10. After you have added all required tasks to the task bundle, click **Save** on the **Edit task bundle** page.

The task bundle is available for transfer. It is displayed on the **Task bundles** page.

## 17 Update Self Service Portal settings

After you have created the task bundles to be transferred when users enroll their devices in the Self Service Portal, you need to update the Self Service Portal settings with the required group settings:

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**, and then click the **Group settings** tab.
2. Click the **Default** group setting.  
The **Edit group settings** dialog box opens.
3. In the **Initial package - corporate devices** and **Initial package - personal devices** lists, select the task bundles you have created for Android and iOS devices.
4. Select the **Active** check box for the platforms that should be available in the Self Service Portal.
5. In the **Add to device group** list, select the group that devices will be added to when they are enrolled in the Self Service Portal.
6. Click **Apply**.
7. On the **Group settings** tab, click **Save**.

## 18 Create a Self Service Portal test user

To test provisioning through the Self Service Portal, create a Self Service Portal user account for yourself. You will use this account to log in to the Self Service Portal and test device enrollment.

### Note

This procedure assumes that the customer was created with internal user management, see [Create a customer](#) (page 9). For information on external user management, see the *Sophos Mobile super administrator guide*.

To create a test user account for the Self Service Portal:

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Create user**.
2. Configure the required account details.  
Make sure that **Send registration email** is selected.
3. Click **Save**.

The user is added to the list of Self Service Portal users and a registration email is sent to the email address that you specified in the account details.

## 19 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 the test user account you created for yourself in [Create a Self Service Portal test user](#) (page 26) and perform test enrollments for all platforms that you want to manage with Sophos Mobile.

## 20 Import users into Sophos Mobile

After you have tested device enrollment through the Self Service Portal, you can import your user list into Sophos Mobile.

The import of users is only relevant for internal user management. For external user management, all users that are assigned to a certain LDAP group can log in to the system.

For information on external user management, see the *Sophos Mobile super administrator guide*.

You add new Self Service Portal users by importing a UTF-8 encoded comma-separated values (CSV) file with up to 300 users.

### Note

Use a text editor for editing the CSV file. If you use Microsoft Excel, values entered may not be resolved correctly. Make sure that you save the file with extension `.csv`.

### Tip

A sample file with the correct column names and column order is available for download from the **Import users** page.

To import users from a CSV file:

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Import users**.
2. On the **Import users** page, select **Send registration emails**.
3. Click **Upload a file** and then navigate to the CSV file that you have prepared. The entries are read in from the file and are displayed.
4. If the data is not formatted correctly or is inconsistent, the file as a whole cannot be imported. In this case, follow the error messages that are displayed next to the relevant entries, correct the content of the CSV file accordingly and upload it again.
5. Click **Finish** to create the user accounts.

The users are imported and displayed on the **Show users** page. They will receive emails with their login credentials for the Self Service Portal.

## 21 Use the device enrollment wizard to assign and enroll new devices

You can easily enroll new devices with the device enrollment 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.

To start the device enrollment wizard:

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

### Tip

Alternatively, you can start the wizard from the **Dashboard** page by clicking the **Add device** widget.

2. On the **Enter user search parameters** wizard page, you can 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.
3. After you have entered search criteria, the wizard displays a list of matching users. Select the required user.
4. On the **Device details** wizard page, configure the following settings:

Option	Description
Platform	The device platform. You can only select a platform that is enabled for the customer that you logged in to.
Name	A unique name under which the device will be managed by Sophos Mobile.
Description	An optional description of the device.
Phone number	An optional phone number. Enter the number in international format, for example +491701234567.
Email address	The email address to which the enrollment instructions are sent. If user management is configured for the customer, this is the email address of the user assigned to the device. If no user management is configured, enter an email address here.
Owner	Select the device owner type: either <b>Corporate</b> or <b>Personal</b> .
Device group	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 <b>Default</b> , which is always available.

5. Select a task bundle that will be transferred to the device after it has been enrolled. Or select **Only enroll device** to enroll the device without transferring a task bundle. When you click **Next**, the device is added to Sophos Mobile.
6. On the **Enrollment** wizard page, follow the instructions to complete the enrollment process.

### Note

On Macs, the enrollment procedure must be performed by the user that will be managed by Sophos Mobile. To install the enrollment profile, the user must enter an administrator password.

7. When enrollment has been completed successfully, click **Finish** to close the device enrollment wizard.

### 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.



## 22 Glossary

customer	The tenant that manages devices.
device	The device to be managed (for example smartphone, tablet or Windows 10 device).
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.
provisioning	The process of installing the Sophos Mobile Control app on a device.
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.
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 through Sophos Mobile.
SMSec	Abbreviation for Sophos Mobile Security.
Sophos Mobile client	The Sophos Mobile Control app that is installed onto devices managed by Sophos Mobile.
Sophos Mobile console	The web interface that you use to manage devices.
Sophos Mobile Security	A security app for Android devices. 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 and iOS devices 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 and iOS devices 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.

## 23 Technical support

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

- Visit the Sophos Community at [community.sophos.com/](https://community.sophos.com/) and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at [www.sophos.com/en-us/support.aspx](https://www.sophos.com/en-us/support.aspx).
- Download the product documentation at [www.sophos.com/en-us/support/documentation.aspx](https://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>.

## 24 Legal notices

Copyright © 2018 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.