SOPHOS

Cybersecurity made simple.

Sophos Mobile

startup guide (on premise)

product version: 9.5

Contents

1 About this document

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

The descriptions apply to on-premise installations of Sophos Mobile.

For other versions of this document, see the Sophos Mobile documentation web page.

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 Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.

For further information, 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 Admin.

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 **First steps** wizard to perform initial configuration of the Sophos Mobile server.

   Note
   The **First steps** 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 iPhones, iPads, and Macs.
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 Configure system settings

When you log in to Sophos Mobile Admin for the first time after installation, the **First steps** wizard assists you in configuring system settings.

You must provide the following:

- The address of your HTTP proxy server (if applicable).
- Your license key for Sophos Mobile.
- Your SSL/TLS certificates.
- The credentials for your SMTP server.

Note
You can change all settings later under **Setup > Sophos setup**.

1. On the **HTTP proxy** page, enter the address and port of a proxy server to be used for outbound HTTP and SSL/TLS connections.
2. On the **License** page, enter your license key or request a trial license:
   - **Standard license key**: Enter your Mobile Standard license key and click **Activate**.
   - **Advanced license key**: Enter your Mobile Advanced license key and click **Activate**. You must enter a Mobile Standard license key first.
   - **Request trial**: Enter the email address you used to download the Sophos Mobile installer from the Sophos website.
3. On the **SSL/TLS** page, configure the SSL/TLS certificates used for securing the connections between the Sophos Mobile server and the clients.
   a) Click **Auto-discover certificate(s)**.
      In most cases the auto-discover function can discover the certificates currently in use.
   b) If the certificates are not discovered automatically, upload them manually: Click **Upload a file** and select the relevant CER or DER encoded certificate file.

   You can configure up to four certificates because, depending on your network architecture, different certificates may be in use for clients connecting from the internet or from your local intranet. 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”).

   CAUTION
   Update the certificate 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. On the **SMTP** page, 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
SMTP host	The SMTP server address.

Option	Description
Connection port	The server port to connect to. **Note** 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.
SMTP user	If required by the SMTP server, enter the name of a user that is allowed to connect.
SMTP password	The password of the SMTP user.
Email originator	The email address that will appear in the **From** field of emails from Sophos Mobile.
Originator name	The author name that will appear in the **From** field. If required, you can configure a different originator name (but not email address) for each customer later on. See the Sophos Mobile administrator help.
Send error emails	Sophos Mobile will send error emails, for example when an APNs certificate expires.
New email recipient	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've configured the SMTP information, click **Send test email** to verify the email configuration.
6. Click **Finish** to complete the **First steps** wizard.

6 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.

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 > Sophos setup**, and then click the **License** tab.
2. Enter your license key in the **Advanced license key** field 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.

On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then 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 **MANAGE**, click **Customers**.
2. Click **Create customer**.
3. On the **Edit customer** page, configure the following settings.

Option	Description
Name	The customer's name.
Description	Text to describe the purpose of the customer account.
Maximum number of licenses	The number of device users and unassigned devices that can be managed for the customer.
Advanced licenses	If selected, the customer can manage Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.
Valid until	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.
Deactivate account	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 **Deactivate account** check box.
Activated platforms	Select the platforms for which devices can be enrolled.
Device privacy settings	Select **Allow users to locate devices** to enable users to locate their devices if they are lost or stolen. Select **Allow admins to locate devices** to enable administrators to locate devices. Select **Show installed apps** to show the installed apps in the device details.
Clone settings	Select the **Settings and packages** check box if you want all policies, bundles, and packages created in the super administrator account to be available in the customer's account.
User directory	Select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile. Choose from: • **None. No SSP, user-specific policies, or LDAP administrators available.**: 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. • **Internal directory**: Use internal user management for Sophos Mobile Admin and the Self Service Portal. For further information, see the Sophos Mobile administrator help.

Option	Description
	• **External LDAP directory**: In addition to internal user management, you can lookup accounts for Sophos Mobile Admin and the Self Service Portal from an LDAP directory. Click **Configure external LDAP** to specify the server details.

4. Select **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

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. Sign in to Sophos Mobile Admin with the administrator account you've created for the new customer.
2. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Personal** tab.
3. Configure the following settings:

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

4. Select **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.

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. Select **Save**.

11.3 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 in the Self Service Portal and 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. Select **Save**.

12 Set Android management mode

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

We recommend you use Android Enterprise.

1. On the menu sidebar, under **SETTINGS**, select **Setup > Android setup** and then the **Android** tab.
2. In **Management mode**, select **Android Enterprise**.
3. Select **Save**.

Next, set up Android Enterprise for your organization.

12.1 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

12.2 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` and your Sophos Mobile customer name. For example:

```
Organization name (Sophos Mobile/Customer name)
```

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.

Note
After you've set up Android Enterprise you can't change the user management mode, for example from internal user management to an external LDAP directory.

13 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.

13.1 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. The signing request file is specific to the current customer.
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.
7. On the **Certificate** page, click **Create certificate on the Apple portal**.

   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. Select **Save**.

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

14 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.

14.1 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
Deny email	Forbid email access.

Option	Description
	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 Sophos Mobile super administrator guide. 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 and iOS devices.
Deny network	Forbid network access. This action can only be taken if the super administrator has configured Network Access Control. See the Sophos Mobile super administrator guide. This action is not available for devices where Sophos Mobile only manages the Sophos container.
Create alert	Trigger an alert. The alerts are displayed on the **Alerts** page.
Transfer task bundle	Transfer a specific task bundle to the device. This action is only available for Android, iOS, macOS and Windows devices. 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.

15 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.

15.1 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. Select **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.

16 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**.
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**.

If you've selected the **Android Enterprise** mode, you must set up Android Enterprise for your organization before you can enroll devices. See the Sophos Mobile administrator help.

17 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 **Android Enterprise full device management**.

   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.

18 Create task bundle for iOS 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 iPhones and iPads:

1. On the menu sidebar, under **CONFIGURE**, select **Task bundles > iOS**.
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.

19 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:

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

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

Option	Description
Display name	The name of the platform settings. In the Self Service Portal, users select an enrollment type by this name.
Description	A description of the platform settings. This description is displayed in the Self Service Portal next to the name.

Option	Description
Owner	The owner mode (corporate or personal) of devices enrolled with this configuration.
Device group	The device group the device is added to.
Enrollment package	Select the Android task bundle you've created.
Terms of use	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.
Post-enrollment text	The text to be displayed in the Self Service Portal after the enrollment. Leave this field empty to display no text.

7. Select **Apply** to add the platform settings to the Self Service Portal configuration.
8. Select **Add > iOS**, 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.

20 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**, select **People**.
2. Click **Create user**.
3. Configure the required account details.
   Make sure that **Send registration email** is selected.
4. Select **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.

21 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.

22 Import users

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 can import up to 500 users.

If you specify a group that doesn't exist, Sophos Mobile creates it.

The CSV file must have the following specification:

- The first row is treated as a header and is not imported.
- Values must be separated by semicolon, not by comma.
- All rows must have the correct number of semicolon characters, even if you leave out optional values.
- The file extension must be `.csv`.
- To ensure that non-English characters are imported correctly, the file must be UTF-8 encoded.

Tip
On the **Import users** page, select **Example CSV** to download a sample file.

To import users from a CSV file:

1. On the menu sidebar, under **MANAGE**, select **People**.
2. Select **Import users**.
3. On the **Import users** page, select **Send registration emails**.
4. Select **Upload a file** and then navigate to the CSV file you've prepared.
   The entries are read in from the file and are displayed.
5. 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.
6. Select **Finish** to create the user accounts.

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

Related information

Sophos Mobile super administrator guide

23 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 from the **Dashboard** page by clicking the **Add device** widget.

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.
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:

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 **Corporate** or **Personal**.
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 **Default**, which is always available.

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.

24 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.
customer	A customer represents a separate management area within Sophos Mobile. You can set up several customers and manage each customer's devices independently. This is also known as *multitenancy*.
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.
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 Mobile console	The web interface that you use to manage devices.
Sophos Intercept X for Mobile	A security app for Android and iOS 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.
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.

25 Support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

26 Legal notices