SOPHOS

Cybersecurity
made
simple.

Sophos Mobile

user help

product version: 8.6

Contents

1 About this help

This help describes how to set up and use the Sophos Mobile Control app and how to use the Sophos Mobile Self Service Portal.

Your organization might have disabled some functions described in this help.

2 About Sophos Mobile

Sophos Mobile is a management tool for mobile devices like smartphones and tablets, and also for PCs running Windows 10 and Macs. It helps to keep corporate data safe by managing apps and security.

Sophos Mobile secures corporate data on your device and ensures that it is compliant with the corporate policies that apply in your company.

With the Self Service Portal you can enroll your device with Sophos Mobile. In addition, you can remotely locate, lock or wipe your device and reset your password without having to contact the helpdesk.

3 Set up Sophos Mobile on your device

Devices can be enrolled easily using the Self Service Portal.

Note

The number of devices you can enroll through the Self Service Portal may be restricted by company policy. In this case, you cannot enroll any further devices after the specified number has been exceeded.

1. On the Self Service Portal, click **Enroll new device**.
2. Follow the instructions to enroll your device with Sophos Mobile.

3.1 Enrollment steps for Android devices

There are two basic enrollment steps:

1. Install the Sophos Mobile Control app on your device.

2. Configure the app on your device.

For detailed instructions, see the email that you received from your organization. If you enroll a device on the Self Service Portal, the instructions are displayed there.

3.2 Enrollment steps for iOS devices

There are two basic enrollment steps:

1. Install the Sophos Mobile Control app on your device.

2. Configure the app on your device.

For detailed instructions, see the email that you received from your organization. If you enroll a device on the Self Service Portal, the instructions are displayed there.

3.3 Enrollment steps for Macs

To enroll a Mac with Sophos Mobile, you must install an enrollment policy.

For detailed instructions, see the email that you received from your organization. If you enroll a device on the Self Service Portal, the instructions are displayed there.

Important

Sophos Mobile manages the user that is logged in to the Mac when the enrollment procedure is performed. This user can't be changed afterward.

Tip
To view the settings applied to your Mac by your company, click **Profiles** under **System Preferences**.

3.4 Enrollment steps for Windows Phone and Windows Mobile devices

There are three basic enrollment steps:

1. Install the Sophos Mobile Control app on your device.

2. Configure the app on your device.

3. Configure the device management agent on your device.

For detailed instructions, see the email that you received from your organization. If you enroll a device on the Self Service Portal, the instructions are displayed there.

3.5 Enrollment steps for Windows computers

To enroll a Windows computer device with Sophos Mobile, you must configure the device management agent on it.

For detailed instructions, see the email that you received from your organization. If you enroll a device on the Self Service Portal, the instructions are displayed there.

4 What to expect after enrollment

Depending on the settings of the configuration profile installed, the following can be expected after you have enrolled your device with Sophos Mobile:

- New applications may be available.

- Your company may have specified apps to be installed on your device. To view and install them, open the Sophos Mobile Control app on your device and tap **Apps**. For further information, see Install apps (page 14).

- Applications like Camera, YouTube or the App Store might no longer be available on the device.

- Your email application may be configured for access to your corporate mail server.

- When your device becomes non-compliant with the company policy (for example due to a non-compliant app installed on it), a Sophos Mobile notification is displayed. (If you are using iOS, see your Apple documentation for further information on how to enable notifications on your device.) In the Sophos Mobile Control app, you can view all violations. For further information, see Display and resolve compliance violations (page 14). You can also view the compliance violations for devices enrolled for you in the Self Service Portal. For further information, see Display compliance violations (page 6).

- If your company has configured App Protection for specific apps on your device, you must create a password when you open a protected app for the first time. You need to enter this password every time you open the protected app afterward or after your device has been locked. In the Sophos Mobile Control app, you can view the protected apps and lock all of them at once. For further information, see Lock protected apps (page 15).

- The Sophos Mobile Control app may ask for your email password.

- On Android devices that support Samsung Knox, you may be asked to accept the Samsung Knox license agreement. This is required to register the Sophos MDM functionality with the device. The Samsung Knox license is free of charge. You do not need a Samsung Knox Workspace or Samsung Knox Premium license.

- If you have created a work profile on your Android device during the enrollment process, Sophos Mobile only manages that profile, not the whole device. It does not access your personal data and apps. For detailed information on work profiles, see the Android enterprise help (external link).

- If you only have enrolled the Sophos container, Sophos Mobile does not access any data outside of the Sophos container, such as your personal data and apps.

Note
If the configuration is removed from the device as a result of unenrollment, all data (email, calendar items and contacts) and managed apps introduced will also be removed.

5 Manage your device with the Self Service Portal

After your device has been enrolled with Sophos Mobile, you use the Self Service Portal to manage it.

5.1 Synchronize device

Note
This feature is not available for certain device types.

On the Self Service Portal, you can manually synchronize your device with your company's Sophos Mobile server.

This is useful, for example, in the following situations:

- Your device has been switched off for a long period of time and therefore has not been synchronized with the server. In this case, your device is non-compliant and you may, for example, not be able to receive emails. To make your device compliant again, you must synchronize it with the Sophos Mobile server.
- Your device is non-compliant due to other reasons (for example, forbidden apps) and you have to make changes on your device to comply with your company policy. After you have made the necessary changes, you must synchronize your device with the Sophos Mobile server.

To manually synchronize your device:

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Refresh data**.

5.2 Display compliance violations

Note
This feature is not available for certain device types.

On the Self Service Portal, you can display compliance violations of your device.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Compliance status**.
   Compliance status is only available when your device is not compliant.

On your device, you must perform the necessary actions to make it compliant.

5.3 Lock device

Note
This feature is not available for certain device types.

You can lock your device if it is lost or stolen.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Lock**.

   For iOS devices, you can enter a message of up to 300 characters that will be displayed on the device after it has been locked. For example, you enter a message with a contact number in case your device is found. In the **Phone number to display** field, you can enter a number that is dialed automatically if somebody taps it in the lock message.

   For Macs, you set a 6-digit PIN that must be entered on the Mac to unlock it.

Your device is locked with your current password or – in the case of a Mac – with the system lock PIN.

5.4 Turn on Lost Mode

Note
This section only applies to iOS devices.

You can put your iOS device into Lost Mode if it is lost or stolen.

In Lost Mode, the only actions available on the device are:

- Dial a phone number you have configured.

- Make an emergency call.

Important
If you turn on Lost Mode in the Self Service Portal, you can't turn it off in iCloud, and vice versa.

To turn on Lost Mode:
1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Turn on Lost Mode**.
3. Configure the following settings:

Option	Description
Lock screen message	Text that is displayed on the lock screen.
Lock screen phone number	A phone number that can be dialed from the lock screen.

Option	Description
Footnote	Footnote text that is displayed at the bottom of the lock screen.
	If you don't configure a footnote, a standard note to contact an administrator is displayed.

4. Confirm the action. Your device is immediately put into Lost Mode.

When your device is in Lost Mode, you can perform the following actions in the Self Service Portal:

- To locate the device, use **Locate**.

- To play a sound on the device, use **Play Lost Mode sound**.

- To turn off Lost Mode, use **Turn off Lost Mode**.

5.5 Reset device password

Note
This feature is not available for certain device types.

You can reset your device password in the Self Service Portal.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions** and then click **Reset password**.
3. Confirm any information messages or follow the instructions that are displayed.

For Android and Windows Mobile, the device is locked with the one-time password displayed in the Self Service Portal. After you've unlocked the device, you must create a new password.

For iOS, the password is removed and the device is unlocked.

Note
- For Android devices where Sophos Mobile only manages a work profile, the **Reset password** action resets the work profile's password.

- For Android enterprise devices with Android 8.x or later, you must turn on the password reset feature in the Sophos Mobile Control app before you can reset the password in the Self Service Portal.

5.6 Reset App Protection password

Note
This section only applies to Android devices.

If your company has configured App Protection for specific apps on your device, you must create a password when you open a protected app for the first time. You must enter the password every time you open the app or after your device has been locked. You can reset the password using the Self Service Portal.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Reset App Protection password**.

3. In the dialog box, enter a new password in the **New password** field and confirm it.
4. Click **Reset password**.

5.7 Reset Sophos container password

Note

This feature is only available if your organization has set up the Sophos container on your device.

You can reset your Sophos container password in the Self Service Portal. This password is used for both, the Sophos Secure Workspace and the Sophos Secure Email app.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Reset Sophos container password**.

Your Sophos Secure container password is removed. You must define a new password.

5.8 Locate device

Note

This feature is not available for certain device types.

You can display the location of your device in Google Maps, for example if it is lost or stolen.

Note

For iOS and Windows Mobile devices, the **Locate** feature is of limited use because you have to confirm messages on the device before the location is displayed.

1. On your device, make sure that location services are turned on and that the Sophos Mobile Control app is allowed to use them.
2. In the Self Service Portal, click **My devices** and then click the relevant device.
3. Click **Actions > Locate**.
   A task is created and sent to the device.
4. In the device details, click **Location** to view the location of your device in Google Maps.

Important

For privacy reasons, the locate action is recorded by your organization.

5.9 Wipe device

Note

This feature is not available for certain device types.

Note
This section does not apply to Android devices where Sophos Mobile only manages a work profile.
To wipe the work profile on these devices, see Wipe Android work profile (page 10).

You can wipe your device, i.e. reset it to its factory settings, if it is lost or stolen. If you are in doubt whether a wipe is required, contact your technical support.

Important
If you wipe your device, all data is deleted. This can't be undone.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Wipe**.

   For Macs, you set a 6-digit PIN that must be entered on the Mac to unlock it after it has been wiped.

Your device is reset to its factory settings. All data is deleted.

5.10 Wipe Android work profile

For Android devices where Sophos Mobile only manages a work profile, you can remove the work profile from your device if it is lost or stolen. This removes all corporate apps and data from the device, including the Sophos Mobile Control app. This does not remove your personal data and apps. Contact your technical support if you are not sure whether you should wipe the Android work profile.

Important
You cannot undo removing the work profile from the device.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Wipe Android work profile**.

The work profile is removed. Your device is no longer enrolled with Sophos Mobile.

5.11 Reconfigure Sophos Mobile device management

If you manually deactivate Sophos Mobile device management on your device, without using the Self Service Portal or the Sophos Mobile Control app, the Self Service Portal still lists the device as managed. To manage the device, you must reconfigure it.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Reconfigure**.
   A message box is displayed, warning you that the device will be unenrolled if it is managed.

The device is triggered to contact the Sophos Mobile server. Depending on how quickly the device responds, it may take some time before the reconfiguration starts.

Perform the enrollment process as described in Set up Sophos Mobile on your device (page 3). After the process has been completed, your device is enrolled with Sophos Mobile again.

5.12 Reconfigure the Sophos Mobile Control app

Note
This section only applies to iOS and Windows Mobile devices.

If the Sophos Mobile Control app has been accidentally uninstalled from your managed device, you need to do the following:

- Reinstall the app.

- Reconfigure the app to connect it to the Sophos Mobile server again.

Note
This section does not apply if the Sophos Mobile device management (MDM) account on the device was also removed. In this case, you must reconfigure the device. See Reconfigure Sophos Mobile device management (page 10).

To reconfigure the Sophos Mobile Control app:

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Reconfigure the SMC app**.
   A page with detailed instructions is displayed.
3. Use the Sophos Mobile Control app to scan the displayed QR code, or enter the displayed configuration details manually.

The Sophos Mobile Control app is reconnected to the Sophos Mobile server.

5.13 Unenroll device

Note
This section does not apply to Android devices where Sophos Mobile only manages a work profile. To unenroll these devices, see Wipe Android work profile (page 10).

On the Self Service Portal, you can unenroll your device from Sophos Mobile. Do this if you no longer use your managed device, for example because you got a new one.

Important
You cannot undo unenrolling the device.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Unenroll**.

Your device is removed from device management. This has the following effects:

- For Android devices:

  — The Sophos Mobile Control device administrator is disabled.

  — If installed, the Sophos Samsung Plugin device administrator is disabled.

  — All data is removed from the app, but the app remains on the device. If required, you have to uninstall the Sophos Mobile Control app manually.

- — The container apps (Sophos Secure Workspace and Sophos Secure Email) and the Sophos Mobile Security app are reset.
- For Android devices, when the device is enrolled with Sophos Mobile Control in Android enterprise device owner mode:
  - — The device is wiped.
- For iPhones and iPads:
  - — The MDM base profile and all further profiles and managed apps installed by Sophos Mobile are removed.
  - — The Sophos Mobile Control app is uninstalled.
  - — Restrictions imposed on the device are lifted.
  - — All accounts configured by Sophos Mobile and associated data are removed. This includes your corporate email.
  - — All apps received from Sophos Mobile (known as *managed apps*) are removed.
  - — All certificates received from Sophos Mobile are removed.
  - — The container apps (Sophos Secure Workspace and Sophos Secure Email) are reset.
- For Macs:
  - — The enrollment policy and other device and user policies installed by Sophos Mobile are removed.
  - — Restrictions imposed on the device are lifted.
  - — All accounts configured by Sophos Mobile and associated data are removed. This includes your corporate email.
  - — All certificates received from Sophos Mobile are removed.
- For Windows Phone and Windows Mobile devices:
  - — The Sophos Mobile Control app and all policies are removed from the device.
  - — The server login data and all other data received from the server are removed.
- For Windows computers:
  - — The Sophos Mobile device management (MDM) account on the device is removed.
  - — The server login data and all other data received from the server are removed.

5.14 Delete unenrolled device

After you have unenrolled or wiped a device, you can delete it in the Self Service Portal to remove it from the system.

1. In the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Actions > Delete**.

The device no longer shows up in the list of your devices.

5.15 Get support

In the menu bar, click **Support**.

The **Support** page is displayed with details how to contact your support team and any further information provided.

6 Manage your device with the Sophos Mobile Control app

After you've enrolled your device with Sophos Mobile, you can perform the tasks described in the following sections in the Sophos Mobile Control app.

For most functions, your device must be connected to the internet.

6.1 Synchronize device

In the Sophos Mobile Control app, you can manually synchronize your device with your company's Sophos Mobile server.

This is useful, for example, in the following situations:

- Your device has been switched off for a long period of time and therefore has not been synchronized with the server. In this case, your device is non-compliant and you may, for example, not be able to receive emails on your device. To make your device compliant again, you must synchronize it with the Sophos Mobile server.

- Your device is non-compliant due to other reasons (for example, forbidden apps) and you have to make changes on your device to comply with your company policy. After you have made the necessary changes, you must synchronize your device with the Sophos Mobile server.

To manually synchronize your device:

- On the dashboard of the Sophos Mobile Control app, tap **Synchronize now**.

6.2 Display and resolve compliance violations

When your device becomes non-compliant with the company policy, for example because you have installed a forbidden app, Sophos Mobile displays a notification on your device.

In the Sophos Mobile Control app, you can display all violations:

1. On the dashboard of the Sophos Mobile Control app, tap the topmost tile that displays the compliance status.

   A list of all compliance violations is displayed.
2. Tap **Fix it**, next to a violation, and follow the necessary steps to resolve the compliance violation.

6.3 Install apps

> **Note**
> For Android devices where Sophos Mobile only manages a work profile, see Install apps in the work profile (page 15).

Your company may have configured apps for your device. You can install these apps directly from the Sophos Mobile Control app.

1. On the dashboard of the Sophos Mobile Control app, tap **Apps**.
2. Tap the app you want to install and then follow the installation procedure.

Note
Depending on your device type, your company may install apps on your device without your confirmation.

6.4 Install apps in the work profile

Note
This section applies to Android devices where Sophos Mobile only manages a work profile.

Your company may have approved apps for your device. You can install these apps from the Google Play Store app in your work profile.

1. On your device, open the Google Play Store app that has a briefcase badge.
2. Browse for the app that you want to install.
3. On the app page, tap **Install** and follow the installation procedure.

Note
Your company may directly install or uninstall apps in the work profile without your confirmation.

6.5 Lock protected apps

Note
This section only applies to Android devices.

If your company has configured App Protection for specific apps on your device, you must create a password when you open a protected app for the first time. Afterward the app is password-protected. You need to enter the password every time you open the app or after your device has been locked. In the Sophos Mobile Control app, you can view the protected apps and lock all of them at once. This is useful, for example, if you want to hand over your device to somebody else, to prevent them from using your protected apps.

Note
You can reset the password using the Self Service Portal.

1. On the dashboard of the Sophos Mobile Control app, tap **App Protection**.
   Under **Protected Apps** all apps your company has configured as protected are shown.
2. Tap **Lock listed apps**.

6.6 Display forbidden apps

Note
This section only applies to Android devices.

Your organization might have defined apps not allowed to start. You can view these apps in the Sophos Mobile Control app:

- On the dashboard of the Sophos Mobile Control app, tap **App Control**.

A list of apps not allowed to start is displayed.

6.7 Display messages from your company

Your company can send messages to your device. When you receive a message, a notification is displayed. You can read the message in the Sophos Mobile Control app.

- On the dashboard of the Sophos Mobile Control app, tap **Messages**.
  All messages that you have received so far are displayed. You can delete individual messages.

Tip
Tap the notification for an incoming message to open the Sophos Mobile Control app.

6.8 Unenroll device

Note
This feature is not available for certain device types.

You can unenroll your device from Sophos Mobile. Unenrolling deletes the server connection and all corresponding data but does not uninstall the Sophos Mobile Control app.

To unenroll your device, open the Sophos Mobile Control app on your device and then perform the following actions:

- For Android:

  a) In the title bar of the dashboard, tap **More** ⋮ and then tap **About**.

  b) In **About**, tap **Unenroll**.

- For iOS:

  a) In the title bar of the dashboard, tap **About** ⓘ, and then tap **Unenroll**.

- For Windows Mobile, using the **Sophos Mobile Control 2017** app:

  a) In the title bar of the dashboard, tap **Support** 🎧.

  b) In the title bar of **Support**, tap **Unenroll** ⊗.

- For Windows Phone and Windows Mobile, using the **Sophos Mobile Control** app:

    a) On the dashboard, tap **Settings**.

    b) At the bottom of **Settings**, tap **More ⦁⦁⦁** and then tap **Unenroll**.

6.9 Get support

In the Sophos Mobile Control app, you can display details how to contact your support team and any further information provided.

- On the dashboard of the Sophos Mobile Control app, tap **Support**.

    Tip
    You can tap the **Email**, **Phone** or **Mobile** field to write an email or make a phone call to your support contact.

7 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.

- 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.

8 Legal notices