## Contents

1. About Sophos Mobile Control ................................................................. 4
2. About this guide ...................................................................................... 5
3. Login to the Self Service Portal ............................................................. 6
   3.1 First login ......................................................................................... 6
   3.2 Login ............................................................................................. 6
   3.3 Password recovery ........................................................................... 6
   3.4 Logout ........................................................................................... 7
4. Setting up Sophos Mobile Control on your device ................................. 8
   4.1 Installation steps for Android devices .......................................... 8
   4.2 Installation steps for iOS devices .................................................. 9
   4.3 Installation steps for Windows Phone devices ............................... 10
5. What to expect after installation ........................................................... 12
6. Using the Sophos Mobile Control app .................................................... 13
   6.1 Synchronize your device manually (Android, iOS, Windows Phone) .... 13
   6.2 Install required and recommended apps (Android, iOS, Windows Phone) .... 13
   6.3 Lock protected apps (Android) ...................................................... 13
   6.4 View apps not allowed to start (Android) ........................................ 14
   6.5 View compliance violations on your device (Android, iOS, Windows Phone) .......... 14
   6.6 View server messages on your device (Android, iOS, Windows Phone) .......... 15
   6.7 Use the Support view (Android, iOS, Windows Phone) ....................... 15
   6.8 Unenroll device (Android, iOS, Windows Phone) ............................. 15
7. Using the Self Service Portal after Sophos Mobile Control setup .......... 16
   7.1 View compliance violations in the Self Service Portal (Android, iOS, Windows Phone) ................................................................. 16
   7.2 Synchronize your device manually (Android, iOS, Windows Phone) ........ 16
   7.3 Lock device (Android, iOS, Windows Phone from 8.1) ....................... 17
   7.4 Reset device password (Android, iOS, Windows Phone from 8.1) ............ 17
   7.5 Reset app protection password (Android) ......................................... 17
   7.6 Reset Sophos Secure Workspace (SSW) app password (iOS, Android) .......... 18
   7.7 Show location of your device (Android, iOS, Windows Phone) .............. 18
   7.8 Wipe device (Android, iOS, Windows Phone) ................................. 19
   7.9 Reconfigure device (Android, iOS, Windows Phone) ......................... 19
1 About Sophos Mobile Control

Sophos Mobile Control is a mobile device management solution for smartphones and tablets. It allows configuration and software distribution as well as security settings and many other device management operations on mobile devices. The Sophos Mobile Control system consists of a server and a client component which communicate through data connections.

Sophos Mobile Control secures corporate data on your mobile device and ensures that your device is compliant with the corporate policy that applies in your company.

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

**Note:** The functions available in the Self Service Portal may vary depending on the system configuration according to company policy. Some functions described in this guide may not be available in your Self Service Portal.
2 About this guide

This guide describes how to

- Install and set up Sophos Mobile Control on Android, Apple iOS and Windows Phone devices
- View messages sent by the server on your device
- View compliance violations on your device and in the Self Service Portal
- Manually synchronize registered devices with the Sophos Mobile Control server
- Lock devices in case of theft or loss
- Reset your device password/passcode
- Reset devices to their factory settings (wipe) in case of theft or loss
- Reconfigure your device if Sophos Mobile Control has been removed from it
- Show the location of devices in case of theft or loss
- Decommission devices and delete them from the list of registered devices in the Self Service Portal
- Reset app protection passwords

Note: The functions available in the Self Service Portal may vary depending on the system configuration according to company policy. Some functions described in this guide may not be available in your Self Service Portal.
3 Login to the Self Service Portal

3.1 First login

**Note:** Depending on the system configuration, the first login procedure may differ from the one described in this section. The procedure described refers to users created through Sophos Mobile Control internal user management. If a different user management method is used, you will receive the required login information from your system administrator.

For login at the Self Service Portal, you will receive the Self Service Portal URL from your system administrator. For the first login, you will also receive a welcome email with your user credentials and a link for activating your account.

To log in at the Self Service Portal for the first time:

1. In the Self Service Portal welcome email, click the link for activating your account.
   
   The Sophos Mobile Control Self Service Portal asks you to define your password.

2. Enter your new password twice and click **Change password**.
   
   You are logged in with your new password and forwarded to the **Home** page.

3.2 Login

1. Go to the Self Service Portal URL.
   
   The Self Service Portal login dialog is displayed.

2. Enter your **Customer** name, **User** name and your **Password** and click **Login**.
   
   You are logged in to the Self Service Portal. The Self Service Portal **Home** page is displayed.

3.3 Password recovery

If you have forgotten your password for logging in to the Sophos Mobile Control Self Service Portal, you can reset it.

1. In the **Login** dialog of the Self Service Portal, click **Forgot password**?
   
   The **Reset password** dialog is displayed.

2. Enter your **Customer** and **User** information and click **Reset password**.
   
   You receive an email with a link for resetting your password.

3. Click the link.
   
   The Sophos Mobile Control Self Service Portal asks you to define your password.
4. Enter your new password twice and click **Change password**.
   You are logged in with your new password and forwarded to the **Home** page.

### 3.4 Logout

To log out from the Self Service Portal, click your user name in the menu bar and select **Logout**.
4 Setting up Sophos Mobile Control on your device

Devices can be enrolled easily using the Self Service Portal. You will be guided through the steps that are also described here for reference.

1. Log in to the Sophos Mobile Control Self Service Portal.

   The Self Service Portal Home page is displayed.

   **Note:** If other devices have been registered for you, they are displayed in a list on the Home page. This list shows all devices you have registered through the Self Service Portal and devices that have been registered for you by your system administrator.

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

2. Click **Register new device**.

   The Company Policy page is displayed.

3. Read the company policy information, select *I accept the terms* and click **Next**.

4. On the **Select the device type** page, select your platform and click **Next**.

5. On the **Select the installation mode** page, select whether you are working from a personal computer or your mobile device that will be registered. Click **Next**.

6. On the **Device information** page, enter your email address and whether it is a company or private device. Click **Next**.

   Further installation instructions are displayed. They depend on the operating system of your device and are also sent as email to the address you provided.

4.1 Installation steps for Android devices

There are two basic steps for installation: first, you install the Sophos Mobile Control app; afterwards, you configure the app on your device. In the email you received you find links and explanations concerning the steps that are also described here in detail.

1. Download and install the app "Sophos Mobile Control" on your mobile device. You can tap the link in the email, or you can search for it in the device’s app store.

   Upon completion a success message is displayed.
2. To configure the app, tap the corresponding link in the email or in the Self Service Portal (if you are working from your device) or start Sophos Mobile Control by tapping the icon on your device’s homescreen.

A button Configure app or a screen with instructions and the options to scan the QR code or manually enter your data is displayed. If you scan the QR code, focus the camera on the QR code displayed by the Self Service Portal or your email until the QR code is recognized. You do not need to tap or press any button. Wait for the configuration to finish.

3. When you are prompted, activate Sophos Mobile Control as a device administrator.

Among other features, Sophos Mobile Control offers you to remotely locate, lock or wipe your device in case of theft or loss. This means that you need to provide the app with extensive rights to change configuration and passwords, delete data and perform a factory data reset without further warning. For this reason you have to activate Sophos Mobile Control as a device administrator.

4. If your device supports Samsung SAFE, you may also be prompted to install the Sophos Mobile Control Samsung SAFE plugin. Tap OK in the message displayed and install the plugin.

5. If your company runs a valid Samsung KNOX license, you will be asked to create a Samsung KNOX container. A KNOX container is a virtual Android environment, isolating apps and data from outside the container. It is a secure company workspace and has its own home screen, launcher, apps, and widgets. Follow the instructions on your device to create the Samsung KNOX container. You will be asked to define your KNOX unlock method, for example a PIN. Depending on your company settings, Exchange ActiveSync will be configured and you may be asked for your Exchange password. After configuration of Exchange ActiveSync open your email app in the KNOX container. Finally, further configuration steps within your KNOX container might be done or you might be required to download and install apps.

Now your Samsung KNOX container is configured and accessible from the Notification Panel.

6. The remainder of the installation and configuration process depends on your company-specific configuration. Depending on the system configuration, you may receive a post-installation message that describes any further required steps. Follow the instructions in the message.

Sophos Mobile Control has been installed and set up on your device.

Your device is added to the Sophos Mobile Control list of registered devices. Change to the Home view in the Self Service Portal to find the entry for the device and manage it.

4.2 Installation steps for iOS devices

There are two basic steps for installation: first, you install the Sophos Mobile Control app; afterwards, you configure the app on your device. In the email you received, you will find links and explanations concerning the steps that are also described here in detail.

1. Download and install the app “Sophos Mobile Control” on your mobile device. You can tap the link in the email, or you can search for it in the device’s app store.
2. To configure the app, tap the corresponding link in the email or in the Self Service Portal (if you are working from your device) or start Sophos Mobile Control by tapping the icon on your device’s homescreen. If you are asked whether you want to receive notifications or allow access to the camera, confirm.

A button Configure app or a screen with instructions and the options to scan the QR code or manually enter your data is displayed. If you scan the QR code, focus the camera on the QR code displayed by the Self Service Portal or your email until the QR code is recognized. You do not need to tap or press any button. When the device is ready for the next step, the Mobile Device Management profile installation page is displayed.

3. Install Mobile Device Management. Confirm any warning messages about what the installation process will do. You may also have to enter your PIN.

4. The remainder of the installation and configuration process depends on your company-specific configuration. Depending on the system configuration, you may receive a post-installation message that describes any further required steps. Follow the instructions in the message. If an app that is required according to your company settings is installed on the device, an additional page may be displayed. On this page, you must confirm the installation of the app.

Sophos Mobile Control has been installed and set up on your device.

Your device is added to the Sophos Mobile Control list of registered devices. Change to the Home view in the Self Service Portal to find the entry for the device and manage it.

4.3 Installation steps for Windows Phone devices

There are three basic steps for installation: first, you configure the native device management agent; then you install the app, and finally you configure the app on your device. In the email you received, you will find links and explanations concerning the steps that are also described here in detail.

1. Download and install the app "Sophos Mobile Control" on your mobile device. You can tap the link in the email, or you can search for it in the device’s app store.

Upon completion a success message is displayed.

2. To configure the app, tap the corresponding link in the email or in the Self Service Portal (if you are working from your device) or start Sophos Mobile Control by tapping the icon on your device’s homescreen.

A button Configure app or a screen with instructions and the options to scan the QR code or manually enter your data is displayed. If you scan the QR code, focus the camera on the QR code displayed by the Self Service Portal or your email until the QR code is recognized. You do not need to tap or press any button. Wait for the configuration to finish.

3. On your device open Settings, select workplace and tap add account.

4. Enter your data as displayed on the screen and in the email you received:
   a) Enter your Email address and tap sign in.
   b) Enter the Server URL and tap sign in.
   c) Enter User name, Password and Domain and tap sign in.
5. The remainder of the installation and configuration process depends on your company-specific configuration. Depending on the system configuration you may receive a post-installation message that describes any further required steps. Follow the instructions in the message.

Sophos Mobile Control has been installed and set up on your device.

Your device is added to the Sophos Mobile Control list of registered devices. Change to the **Home** view in the Self Service Portal to find the entry for the device and manage it.
5 What to expect after installation

Depending on the settings of the configuration profile installed, the following can be expected after installation:

- New applications may be available.
- Your system administrator may have specified required and recommended apps to be installed on your device. To view and install them, open Sophos Mobile Control on your device and tap on **Required** or **Recommended**. For further information, see Install required and recommended apps (Android, iOS, Windows Phone) (page 13).
- Applications like Camera, YouTube or the App Store might no longer be available on the device.
- Your email application may be preconfigured 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 Control 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 View compliance violations on your device (Android, iOS, Windows Phone) (page 14). You can also view the compliance violations for devices registered for you in the Self Service Portal. For further information, see View compliance violations in the Self Service Portal (Android, iOS, Windows Phone) (page 16).
- If your system administrator has configured app protection for specific apps on your device, you will be prompted to define 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 afterwards 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 (Android) (page 13).
- If a TouchDown email client is available on your Android device, it will be configured as your primary email client.
- The Sophos Mobile Control app may ask for your email password.

**Note:** If the configuration is removed from the mobile device as a result of decommissioning, all data (email calendar items and contacts) and managed apps introduced will also be removed.
6 Using the Sophos Mobile Control app

After your device has been registered with Sophos Mobile Control and the Sophos Mobile Control app has been installed on your device, you can carry out the procedures described in the following sections in the Sophos Mobile Control app. For most functions it is necessary that the device has a working internet connection.

6.1 Synchronize your device manually (Android, iOS, Windows Phone)

After you have installed and configured the software on your device, you can manually synchronize it with the Sophos Mobile Control 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 have to synchronize it with the Sophos Mobile Control server.

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

To manually synchronize your device:

1. Open the Sophos Mobile Control app on your device.
2. In the Home view, tap Synchronize now.

6.2 Install required and recommended apps (Android, iOS, Windows Phone)

Your system administrator may have configured required and recommended apps for your device. You can install these apps directly from the Sophos Mobile Control app.

1. Open the Sophos Mobile Control app on your device.
2. Tap on Apps.

Depending on the system configuration, apps are suggested for installation or installed directly on your device. The installation process depends on the system configuration.

6.3 Lock protected apps (Android)

If your system administrator has configured app protection for specific apps on your device, you will be prompted to define a password when you open a protected app for the first time. Afterwards
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:** The Sophos Mobile Control Self Service Portal offers a function for resetting the password for protected apps. For further information, see Reset app protection password (Android) (page 17).

1. Open the Sophos Mobile Control app on your device.
2. Tap on **App protection**.
   
   Under **Protected Apps** all apps your system administrator has configured as protected are shown.
3. Tap **Lock listed apps**.

### 6.4 View apps not allowed to start (Android)

If your system administrator has configured **App control** for specific apps on your device, you cannot start these apps on your device. In the Sophos Mobile Control app, you can view the apps that cannot be started.

1. Open the Sophos Mobile Control app on your device.
2. Tap on **App Control**.
   
   Under **App Control**, you can see a list of all apps that are not allowed to start.

### 6.5 View compliance violations on your device (Android, iOS, Windows Phone)

As soon as your device becomes non-compliant with the company policy (for example, due to a non-compliant app installed on it), a Sophos Mobile Control notification is displayed on your device. These are push messages on iOS and push notifications on Windows Phone and Android.

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

1. Open Sophos Mobile Control on your device.
2. Tap on the compliance status. It is displayed on the top.
   
   A list of all compliance violations is displayed. For some compliance violations, there is a detail view offering more information. Tap the violation to display the detail view. You can now carry out the necessary steps to make your device compliant again.
6.6 View server messages on your device (Android, iOS, Windows Phone)

After Sophos Mobile Control has been installed and set up on your device, you can view messages sent by the Sophos Mobile Control server directly on your device.

1. Open Sophos Mobile Control on your device.
2. Tap on Messages.

The server messages are displayed in the Messages view. You can delete messages from this view.

Note: The notification that a message was received is also displayed on your device when it comes in. Tap the notification to go directly to the Sophos Mobile Control app. If you use the Sophos Mobile Control app with an SMC 4 server, toast notifications that you missed won’t appear in the SMC apps Messages view but will only be kept in the Action Center.

6.7 Use the Support view (Android, iOS, Windows Phone)

The Sophos Mobile Control app offers a Support view that shows support information.

To use the Support view:

1. Open Sophos Mobile Control on your device.
2. Tap on Support.

The Support view is displayed with support contact information. You can use this view to contact your company’s technical support directly.

6.8 Unenroll device (Android, iOS, Windows Phone)

On an Android or iOS device, you can unenroll your device from the About view of Sophos Mobile Control:

- To open the About view on an Android device, tap the menu button at the upper right or at the bottom of the Home view.
- To open the About view on an iOS device, tap the Information button in the navigation bar of the Home view.

The About view shows information about the Sophos Mobile Control version installed on your device and provides a link to the Sophos website.

You can find the Unenroll button at the bottom of this page. Unenrolling deletes the server connection and all corresponding data but does not uninstall the Sophos Mobile Control app.

On a Windows Phone you can find the Unenroll button on the Settings view. The Settings view is accessible tapping the menu button at the bottom of the Home view.
7 Using the Self Service Portal after Sophos Mobile Control setup

After your device has been registered with Sophos Mobile Control and the Sophos Mobile Control app has been installed on your device, you can carry out the procedures described in the following sections in the Self Service Portal. For most functions it is necessary that the device has a working internet connection.

7.1 View compliance violations in the Self Service Portal (Android, iOS, Windows Phone)

You can view all compliance violations for devices registered for you in the Self Service Portal.

**Prerequisites:**
- Your system administrator has activated this function for the Self Service Portal.
- Compliance violations have occurred on your device. Otherwise, this action is not displayed in the Self Service Portal.

1. On the Home page of the Self Service Portal, go to the relevant device in the table of registered devices.
2. Select Show compliance violations from the Select an action dropdown list.

A table with all violations for the selected device shows the violation and the date and time it was detected. You can now carry out the necessary steps to make your device compliant again.

7.2 Synchronize your device manually (Android, iOS, Windows Phone)

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

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.
To manually synchronize your device:
1. Go to the relevant device on the Self Service Portal Home page.
2. Select Refresh data from the Select an action dropdown list.

### 7.3 Lock device (Android, iOS, Windows Phone from 8.1)

In case of theft or loss you can lock your registered device.

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.
1. Go to the Self Service Portal Home page.
2. In the list of registered devices, go to the relevant device.
3. Select Lock from the Select an action dropdown list.
   
   If you use iOS 7 or later, you can enter a lock 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.
4. Confirm that you want to lock the device.
   
   Your device is locked with your current password.

### 7.4 Reset device password (Android, iOS, Windows Phone from 8.1)

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

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.
1. Go to the Self Service Portal Home page.
2. In the list of registered devices, go to the relevant device.
3. Select Reset password from the Select an action dropdown list.
4. Confirm any information messages or follow the instructions that are displayed.
   
   If you use Android or Windows Phone, a new password is created for you automatically and displayed in the Self Service Portal. On iOS, you enter the new password that will be used to lock the device.
   
   Your device is locked and can be unlocked with the new password that has been defined.

### 7.5 Reset app protection password (Android)

If your system administrator has configured app protection for specific apps on your device, you will be prompted to define a password when you open a protected app for the first time. You need to enter the password every time you open the app or after your device has been locked. You can reset the password in the Self Service Portal.
1. Go to the Self Service Portal Home page.
2. In the list of registered devices, go to the relevant device.
3. Select **Reset app protection password** from the **Select an action** dropdown list. A message box is displayed.
4. Enter a new password in the **New password** field and confirm it.
5. Click **Reset password**.

### 7.6 Reset Sophos Secure Workspace (SSW) app password (iOS, Android)

You can remotely reset your Sophos Secure Workspace app password in the Self Service Portal.

1. Go to the Self Service Portal **Home** page.
2. In the list of registered devices, go to the relevant device.
3. Select **Reset SSW app password** from the **Select an action** dropdown list. A message box is displayed informing you that you will need to enter a new password on the device.
4. Select **I am aware that the following action cannot be undone** and click **Reset SSW app password**.

Your Sophos Secure Workspace app password is removed. You are prompted to define a new password.

### 7.7 Show location of your device (Android, iOS, Windows Phone)

In case of theft or loss you can locate your registered device based on GPS coordinates.

**Prerequisites:**

- Your system administrator has activated this function for the Self Service Portal.
- For this function, location services using GPS or wireless networks need to be allowed for your device.

1. Go to the Self Service Portal **Home** page.
2. In the list of registered devices, go to the relevant device.
3. Select **Show location** from the **Select an action** dropdown list. A message box is displayed showing the last location.
4. To show the last known location, click **Show Location**.

On iOS and Windows Phone devices, it is necessary to confirm messages on the device before the location can be displayed.

After the task has been completed, you can view the location of your device in Google Maps.
### 7.8 Wipe device (Android, iOS, Windows Phone)

In case of theft or loss you can reset your registered device to its factory settings (wipe). If you are in doubt whether a full wipe is required, contact your system administrator.

**Note:** If you wipe your device, all data on the device is deleted.

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.

1. Go to the Self Service Portal **Home** page.
2. In the list of registered devices, go to the relevant device.
3. Select **Wipe** from the **Select an action** dropdown list.
   - A message box is displayed, warning you that a factory reset will be performed on the device and this can't be undone.
4. Select **Confirm**.

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

### 7.9 Reconfigure device (Android, iOS, Windows Phone)

If Sophos Mobile Control has been removed from your device (for example, because the device has been wiped) and your device is still registered, you can reconfigure your device with the Self Service Portal. You can select **Reconfigure device** even if Sophos Mobile Control has not yet been removed from the device. Then it will be decommissioned in a first step.

**Note:**

If you want to reconfigure a Windows Phone 8 device, you must first delete the Sophos Mobile Control **workplace** account. You can find the Sophos Mobile Control Account in **Settings > workplace**.

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.

1. Go to the Self Service Portal **Home** page.
2. In the list of registered devices, go to the relevant device.
3. Select **Reconfigure** from the **Select an action** dropdown list.
   - A message box is displayed, warning you that the device will also be decommissioned if it is managed.
4. Click **Confirm**.

The installation and configuration process is initiated. The steps are identical to those described in **Setting up Sophos Mobile Control on your device** (page 8), starting with the **Select the installation mode** page. After the process has been completed, Sophos Mobile Control is set up again on your device.

### 7.10 Decommission device (Android, iOS, Windows Phone)

If you no longer use your managed device, for example because you got a new one, you can decommission it.
This is particularly useful if the number of devices you can register in the Self Service Portal is limited.

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.

To decommission a managed device:
1. Go to the Self Service Portal Home page.
2. In the list of registered devices, go to the relevant device.
3. Select **Decommission** from the **Select an action** dropdown list.
   - A message box is displayed, warning you that this will remove any changes applied by Sophos Mobile Control and this can't be undone.
4. Click **Confirm**.

Your device is removed from device management:

When an **Android** device is removed from device management, then:
- The Sophos Mobile Control device administrator is disabled.
- If installed, the Samsung SAFE 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.

When an **iOS** device is removed from device management, then:
- The MDM base profile and all further profiles and managed apps installed through Sophos Mobile Control are removed.
- The Sophos Mobile Control app is uninstalled.
- Restrictions imposed on the device are lifted.
- The email account configured through Sophos Mobile Control is removed with all emails.

When an **Windows Phone** device is removed from device management, then:
- 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.

### 7.10.1 Delete decommissioned device (Android, iOS, Windows Phone)

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

**Prerequisite:** Your system administrator has activated this function for the Self Service Portal.

1. Go to the Self Service Portal Home page.
2. In the list of registered devices, go to the relevant device.
3. Select **Delete** from the **Select an action** dropdown list.
   - A message box is displayed, warning you that the deletion cannot be undone.
4. Click **Confirm**.
The device no longer shows up in the list of your devices.

7.11 Support information in the Self Service Portal

If any problems occur while using the Self Service Portal that require assistance from your support team, click Support in the header. In the Support view, you can find the contact information for your support team and any further information provided.
8 Technical support

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

- Visit the SophosTalk community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
9 Legal notices

Copyright © 2011 - 2015 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 is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.