Contents

1 About this help..........................................................................................................................4
2 About Sophos Mobile Control...................................................................................................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 Log out................................................................................................................................7
4 Set up Sophos Mobile Control on your device.........................................................................8
   4.1 Enrollment steps for Android devices.........................................................................8
   4.2 Enrollment steps for iOS devices................................................................................9
   4.3 Enrollment steps for Windows Phone and Windows Mobile devices........................10
   4.4 Enrollment steps for Windows Desktop devices.......................................................11
5 What to expect after enrollment..............................................................................................12
6 Manage mobile devices with the Mobile Control app.............................................................13
   6.1 Synchronize device...................................................................................................13
   6.2 Display and resolve compliance violations...............................................................13
   6.3 Install apps................................................................................................................14
   6.4 Install work apps.......................................................................................................14
   6.5 Lock protected apps.................................................................................................14
   6.6 Display apps not allowed to start..............................................................................15
   6.7 Display messages from your company.................................................................15
   6.8 Unenroll device.........................................................................................................15
   6.9 Display technical support contact details..................................................................16
7 Manage mobile devices with the Self Service Portal..............................................................17
   7.1 Synchronize device....................................................................................................17
   7.2 Display compliance violations..................................................................................17
   7.3 Lock device................................................................................................................17
   7.4 Reset device password..............................................................................................18
   7.5 Reset App Protection password...............................................................................18
   7.6 Reset Sophos container password............................................................................18
   7.7 Locate device.............................................................................................................19
   7.8 Wipe device...............................................................................................................19
7.9 Wipe Android for Work...........................................................................................................19
7.10 Reconfigure Sophos Mobile Control..................................................................................20
7.11 Unenroll device...................................................................................................................20
7.12 Delete unenrolled device......................................................................................................21
7.13 Display technical support contact details.........................................................................21
8 Technical support....................................................................................................................22
9 Legal notices..........................................................................................................................23
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 Control Self Service Portal.

**Note:** The functions available on the Self Service Portal may vary depending on the system configuration that is specific to your company. Some functions described in this help may not be available to you.
2 About Sophos Mobile Control

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

The Sophos Mobile Control system consists of a server and a client component.

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

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

For login at the Self Service Portal, you will receive the web address of the Self Service Portal from your company. For the first login, you will also receive a welcome email with your user credentials and a link for activating your account.

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

**Note:** Your company can display messages in the login dialog, for example regarding upcoming upgrades or outage times. Click the message to display its entire content.

1. Open the web address of the Self Service Portal in your web browser.
2. In the login dialog, enter your credentials, then 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 credentials and click **Reset password**.
   You receive an email with a link for resetting your password.
3.4 Log out

To log out from the Self Service Portal, click your user name in the menu bar and select **Logout**.
4 Set 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.

**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 Control.

4.1 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.

On the Self Service Portal or in the email you received, you find links and explanations concerning the steps that are also described here in detail.

To install and configure Sophos Mobile Control on your Android device:

1. Download and install the Sophos Mobile Control app on your mobile device. If you are reading the enrollment email on your device or if you are using the Self Service Portal from your device, you can tap the link in the email or the Self Service Portal. Upon completion a success message is displayed.

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

   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 if it is lost or stolen. 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 Knox, you may also be prompted to install the Sophos Samsung Plugin app. Tap **OK** in the message displayed and install the plugin.
5. If your company runs a valid Samsung Knox Premium 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 enrollment 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.

On the Self Service Portal, your device is added to the list of enrolled devices.

### 4.2 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.

On the Self Service Portal or in the email you received, you find links and explanations concerning the steps that are also described here in detail.

To install and configure Sophos Mobile Control on your iOS device:

1. Download and install the Sophos Mobile Control app on your mobile device. If you are reading the enrollment email on your device or if you are using the Self Service Portal from your device, you can tap the link in the email or the Self Service Portal 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 on the Self Service Portal (if you are working from your device) or start Sophos Mobile Control by tapping the icon on your device’s Home screen. If you are asked whether you want to receive notifications or allow access to the camera, confirm.

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 enrollment 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.
On the Self Service Portal, your device is added to the list of enrolled devices.

4.3 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.

On the Self Service Portal or in the email you received, you find links and explanations concerning the steps that are also described here in detail.

To install and configure Sophos Mobile Control on your Windows Phone or Windows Mobile device:

1. Download and install the Sophos Mobile Control app on your mobile device. If you are reading the enrollment email on your device or if you are using the Self Service Portal from your device, you can tap the link in the email or the Self Service Portal.

   Upon completion a success message is displayed.

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

   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. Connect your device to the Sophos Mobile Control server. Depending on your device type, perform one of the following actions:

   - For Windows 10 Mobile version 1607 or higher: Open Settings > Accounts > Access work or school and then tap Enroll only in device management.
   - For Windows 10 Mobile below version 1607: Open Settings > Accounts > Work access and then tap Enroll in to device management.
   - For Windows Phone 8.1: Open Settings > Accounts > Work access and then tap Connect.
   - For certain patch versions of Windows 10, none of the paths mentioned before are available. In this case, enter the address ms-device-enrollment:?mode=mdm in Microsoft Edge. You might need to confirm a notification to launch the Microsoft account application.

4. Enter your data as displayed on the screen and in the email you received.

5. The remainder of the enrollment 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.
On the Self Service Portal, your device is added to the list of enrolled devices.
4.4 Enrollment steps for Windows Desktop devices

1. On the device that you want to enroll with Sophos Mobile Control, open the dialog to enroll with a device management system.
   The procedure to open that dialog depends on your version of Windows 10:
   - On Windows 10 version 1607 or higher, open Settings > Accounts > Access work or school and then click Enroll only in device management.
   - On Windows 10 below version 1607, open Settings > Accounts > Work access and then click Enroll in to device management.
   - For certain patch versions of Windows 10, none of the paths mentioned before are available. In this case, enter the address ms-device-enrollment:?mode=mdm in Microsoft Edge. You might need to confirm a notification dialog to launch the Microsoft account application.

2. Enter your data as displayed on the screen and in the email you received.
3. The remainder of the enrollment 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.

On the Self Service Portal, your device is added to the list of enrolled devices.
5 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 Control:

- 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 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 Display and resolve compliance violations (page 13). 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 17).
- If your company has configured App Protection for specific apps on your device, you must 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 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 14).
- The Sophos Mobile Control app may ask for your email password.
- If you have enrolled your device with Android for Work, a work profile has been created. Mobile Control manages that profile. It does not access your personal data and apps. For detailed information on Android for Work, see the Android enterprise Help (external link).

**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.
6 Manage mobile devices with the Mobile Control app

After your device has been enrolled with Sophos Mobile Control and the Sophos Mobile Control app has been installed onto your device, you can carry out the procedures 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

**Note:** This section does not apply to Windows Desktop devices.

In the Sophos Mobile Control app, you can manually synchronize your device 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 must synchronize it with the Sophos Mobile Control 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 Control server.

To manually synchronize your device:

1. Open the Sophos Mobile Control app on your device.
2. On the dashboard, tap **Synchronize now**.

6.2 Display and resolve compliance violations

**Note:** This section does not apply to Windows Desktop devices.

As soon as your device becomes non-compliant with the company policy (for example, due to a forbidden app installed on it), Sophos Mobile Control displays a notification on your device.

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

1. Open the Sophos Mobile Control app on your device.
2. On the dashboard, tap the topmost tile that displays the compliance status.
   A list of all compliance violations is displayed.
3. Tap **Fix it**, next to a violation, and follow the necessary steps to resolve the compliance violation.
6.3 Install apps

**Note:** This section does not apply to Windows Desktop devices.

**Note:** For Android devices that are enrolled with Android for Work, see [Install work apps](#) (page 14).

Your company may have configured 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. On the dashboard, tap **Apps**.
3. Tap the app you want to install and then follow the installation procedure.

**Note:** Depending on your device type, your company may directly install apps on your device with or without your confirmation.

6.4 Install work apps

**Note:** This section only applies to Android devices that are enrolled with Android for Work.

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

1. On your device, tap 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 work apps on your device 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 define 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. Open the Sophos Mobile Control app on your device.
2. On the dashboard, tap **App Protection**.

   Under **Protected Apps** all apps your company has configured as protected are shown.

3. Tap **Lock listed apps**.
6.6 Display apps not allowed to start

**Note:** This section only applies to Android devices.

If your company 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 display the apps that cannot be started.

1. Open the Sophos Mobile Control app on your device.
2. On the dashboard, tap **App Control**.

Under **App Control**, you can see a list of all apps that are not allowed to start.

6.7 Display messages from your company

**Note:** This section does not apply to Windows Desktop devices.

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.

1. Open the Sophos Mobile Control app on your device.
2. On the dashboard, 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.

**Note:** If your company uses Sophos Mobile Control 4, you must confirm the notification before a message appears in **Messages**.

6.8 Unenroll device

**Note:** This section does not apply to devices that are enrolled with Android for Work. To unenroll these devices, see **Wipe Android for Work** (page 19).

**Note:** Your company might have turned this feature off.

You can use the Sophos Mobile Control app to unenroll your device from Sophos Mobile Control. 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:
  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 (Legacy) app:
  a) On the dashboard, tap Settings.
  b) At the bottom of Settings, tap More and then tap Unenroll.

6.9 Display technical support contact details

**Note:** This section does not apply to Windows Desktop devices.

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

1. Open the Sophos Mobile Control app on your device.
2. On the dashboard, 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 Manage mobile devices with the Self Service Portal

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

7.1 Synchronize device

Note: Your company might have turned this feature off.

On the Self Service Portal, you can manually synchronize your device 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, 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 have to synchronize your device with the Sophos Mobile Control server.

To manually synchronize your device:
1. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click Refresh data.

7.2 Display compliance violations

Note: Your company might have turned this feature off.

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

7.3 Lock device

Note: This section does not apply to Windows Desktop devices.

Note: Your company might have turned this feature off.
You can lock your device if it is lost or stolen.

1. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click 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.

Your device is locked with your current password.

7.4 Reset device password

Note: This section does not apply to Windows Desktop devices.

Note: Your company might have turned this feature off.

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

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

On Android, Windows Mobile and Windows Desktop devices, a new password is created for you automatically and displayed on 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

Note: This section only applies to Android devices.

If your company has configured App Protection for specific apps on your device, you must define 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. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click 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.

7.6 Reset Sophos container password

Note: This feature is only available if your administrator has installed a Sophos container on your device.
You can remotely 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. On the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Select an action** and then click **Reset Sophos container password**.

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

### 7.7 Locate device

**Note:** Your company might have turned this feature off.

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 usability 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. On the Self Service Portal, click **My devices** and then click the relevant device.
3. Click **Select an action** and then click **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.

### 7.8 Wipe device

**Note:** This section does not apply to devices that are enrolled with Android for Work. To wipe Android for Work on these devices, see **Wipe Android for Work** (page 19).

**Note:** Your company might have turned this feature off.

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. On the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Select an action** and then click **Wipe**.

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

### 7.9 Wipe Android for Work

**Note:** Your company might have turned this feature off.

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 private data and apps. Contact your technical support if you are not sure whether you should wipe Android for Work.
Important: You cannot undo removing the work profile from the device.

1. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click Wipe Android for Work.

The work profile is removed. Your device is no longer enrolled with Android for Work or Sophos Mobile Control.

7.10 Reconfigure Sophos Mobile Control

Note: Your company might have turned this feature off.

If Sophos Mobile Control has been removed from your device (for example, because the device has been wiped) but your device is still enrolled, you can reconfigure your device on the Self Service Portal. The device will be unenrolled and the enrollment process starts again.

1. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click Reconfigure.

A message box is displayed, warning you that the device will also be unenrolled if it is managed.

The device is triggered to contact the Sophos Mobile Control 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 Control on your device (page 8). After the process has been completed, your device is enrolled with Sophos Mobile Control again.

7.11 Unenroll device

Note: This section does not apply to devices that are enrolled with Android for Work. To unenroll these devices, see Wipe Android for Work (page 19).

Note: Your company might have turned this feature off.

On the Self Service Portal, you can unenroll your device from Sophos Mobile Control. 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. On the Self Service Portal, click My devices and then click the relevant device.
2. Click Select an action and then click Unenroll.

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 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.
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 a Windows Phone or Windows Mobile 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.

When a Windows Desktop device is removed from device management, then:

- The Sophos Mobile Control device management (MDM) account on the device is removed.
- The server login data and all other data received from the server are removed.

7.12 Delete unenrolled device

**Note:** Your company might have turned this feature off.

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

1. On the Self Service Portal, click **My devices** and then click the relevant device.
2. Click **Select an action** and then click **Delete**.

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

7.13 Display technical support contact details

On the Self Service Portal, you can display details how to contact technical support and any further information provided.

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

The **Support** page is displayed with details how to contact technical support and any further information provided.
8 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.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
9 Legal notices

Copyright © 2011 - 2017 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 Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.