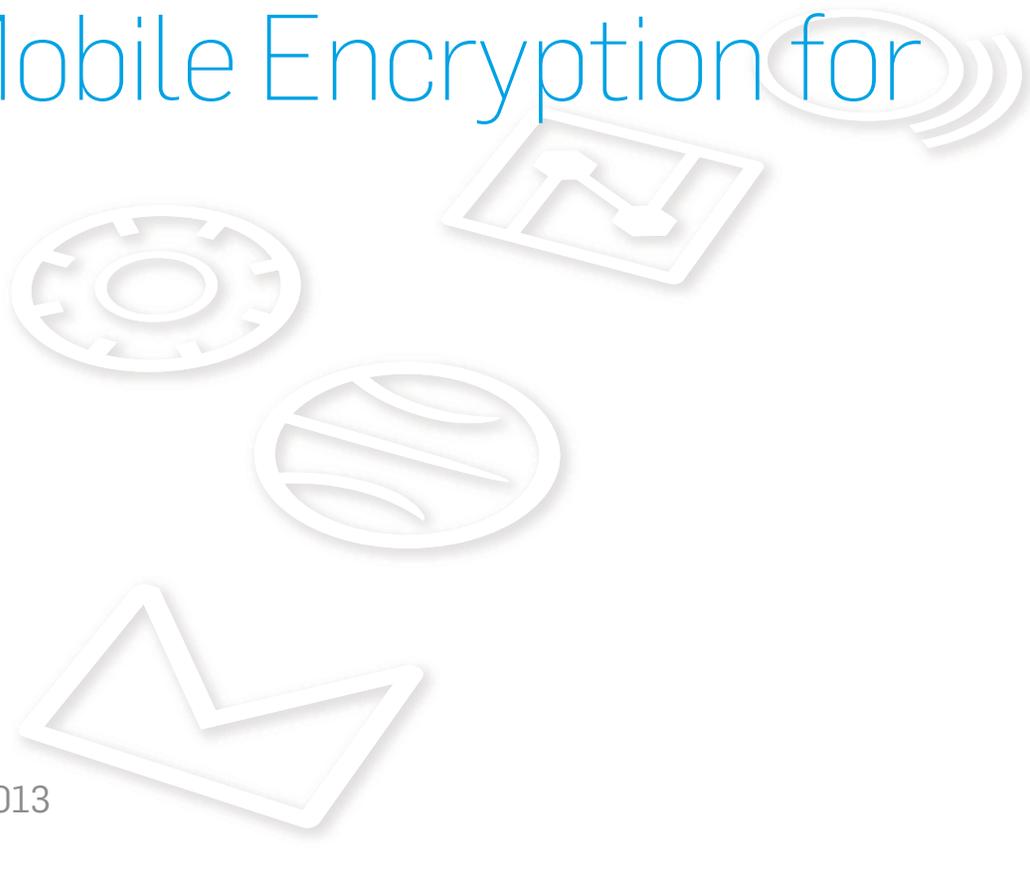


Sophos Mobile Encryption for Android Help

Product version: 1.3
Document date: February 2013



Contents

1 About Sophos Mobile Encryption.....	3
2 Home view	4
3 Local storage.....	5
4 Dropbox.....	6
5 Egnyte.....	8
6 Media Center.....	9
7 Google Drive.....	10
8 Link an account using WebDAV	11
9 Favorites.....	12
10 Technical support.....	14
11 Copyright.....	15

1 About Sophos Mobile Encryption

Sophos Mobile Encryption is an app for Android devices to view Sophos SafeGuard encrypted files stored in Dropbox, Egnyte, Google Drive, Media Center and the local file system. Additionally it provides support for cloud storage providers that provide access via the WebDAV protocol.

With Sophos Mobile Encryption you can read files encrypted by SafeGuard Cloud Storage or SafeGuard Data Exchange. Both are modules of SafeGuard Enterprise or one of its different editions. They allow to encrypt files using a local key. These local keys are derived from a passphrase that is entered by a user. You can only decrypt a file when you know the passphrase that was used to encrypt the file.

For details on the SafeGuard Cloud Storage and SafeGuard Data Exchange modules please refer to the SafeGuard Enterprise 6 documentation on www.sophos.com.

The Sophos Mobile Encryption app is available from Google Play for free.

Sophos Mobile Encryption works on all devices with Android 2.2 and newer.

1.1 Encrypted files on Android devices

Files are encrypted on a Windows endpoint that runs SafeGuard Enterprise or one of its editions first. Then you can transfer them to your Android devices.

Depending on how you want to transfer your encrypted files to your Android device you have to choose the encryption module on the Windows endpoint:

- SafeGuard Cloud Storage encrypts files stored in Dropbox, Egnyte, Google Drive, Media Center, ...

With SafeGuard Cloud Storage and one of these cloud storage providers you can exchange files with partners in an easy, but secure way. You can store encrypted files in the cloud and your partners can read them with Sophos Mobile Encryption. Your partners only have to download it from Google Play first and they need to know the passphrase for the file.

- With SafeGuard Data Exchange you can encrypt single files on the Windows endpoint and transfer them to your Android device in the usual way.

Note: Files encrypted with a *non-local key*, that is a key that has not been derived from a passphrase, cannot be decrypted by Sophos Mobile Encryption.

1.2 Installation and update

You can install the Sophos Mobile Encryption app from Google Play. Update works via the usual mechanism for Android apps.

2 Home view

Tap the **Encryption** icon to start the app. The **Home** view lists the supported storage providers:

- **Favorites:** Opens a view listing the files marked as favorites in the Dropbox view.
- **Local Storage:** Opens a view listing files on the storage card and/or connected external storage.
- **Dropbox:** Opens a view that lists the files in your Dropbox space. Tap the **Link** icon to link to or unlink from Dropbox.
- **Egnyte:** Opens a view that lists the files in your Egnyte space. Tap the **Link** button to open the **Egnyte** configuration dialog.
- **Google Drive:** Opens a view that lists the files in your Google Drive space. Tap the **Link** button to choose an existing Google account or to add a new one.
- **Media Center:** Opens a view that lists the files in your Media Center space. Tap the **Link** button to open the **Media Center** configuration dialog.
- **WebDAV:** Opens a configuration dialog to link with any cloud storage provider that allows access using the WebDAV protocol.

After selecting one of the above, tap the **Up** button in the upper left corner to return to the **Home** view.

Tap the **Back** button of the Android device to return to the previous level. Tap the button twice in the **Home** view to leave the app.

Note: You can select which cloud storage providers are displayed in the **Home** view. To do so tap the **Menu** button and select **Settings**. In the **Cloud storage providers** section select accounts to be displayed. If you de-select an account, it will be hidden. No data is deleted but the account is not synchronized anymore. If you select it again, the account and related data will be displayed again.

3 Local storage

To view encrypted files in local storage on your Android device, the files have to be encrypted on a Windows endpoint that runs SafeGuard Data Exchange first. To enable an endpoint to encrypt files and then transfer them to your Android device, it needs a **policy of type Device Protection with file-based encryption** that allows you to encrypt files with a local key.

As soon as the files are encrypted, you can transfer them to your Android device.

3.1 File list view

Tap **Local Storage** in the **Home** view to list all data in local storage of your Android device.

3.2 View a file

1. Tap a file in the file list view.
2. If the file is encrypted, the **Encryption** app asks you for a passphrase. Enter the passphrase that was used in SafeGuard Enterprise to create the local key for encrypting the file. If you enter a wrong passphrase, a delay of three seconds is imposed before you can retry to enter the passphrase.
3. Tap the **Decrypt** button (checkmark on the right side of the action bar) or the **Done** key on the virtual keyboard.
4. The plain file is forwarded to the associated viewer app. Note that some viewer apps offer editing of documents. As Sophos Mobile Encryption is intended for reading documents only, such changes are lost. They will not be forwarded to the (encrypted) original file.

Note:

You can cancel an ongoing decryption process by pressing the **X** button or tapping the left button in the title bar, switching back to the file list. When you cancel decryption, the partially written plain file is deleted.

4 Dropbox

To view encrypted files in **Dropbox** on an Android device, files in the cloud storage have to be encrypted on a Windows endpoint that runs SafeGuard Cloud Storage first.

To enable an endpoint to encrypt files in **Dropbox** it needs a **policy of type Device protection** with **file based encryption** and **Cloud Storage as target** that allows you to encrypt files in **Dropbox**.

Sophos Mobile Encryption then allows you to view the encrypted files stored in **Dropbox** on your Android device.

4.1 Configure Dropbox

The configuration dialog is displayed if you tap **Dropbox** in the **Home** view and **Dropbox** has not been configured yet.

Tap the **Link/unlink** icon on the right hand side of the **Dropbox** list entry to link or unlink a Dropbox account with Sophos Mobile Encryption.

- **If a Dropbox account has already been linked**, the account info and the **Unlink** icon to unlink the account are displayed. Tap the button to unlink the account.
- **If no Dropbox account is linked**, tap the **Link** icon to trigger the linking of an **Dropbox** account.

4.2 Link a Dropbox account to the app

When you tap the **Link** icon, either the mobile Internet browser or the original **Dropbox** app is launched.

- **Mobile Internet browser**: The **Dropbox** website loads. Here you are asked to log in to **Dropbox**. After login, you are asked if access for **Sophos Mobile Encryption** should be granted.
- **Original Dropbox app**: The original **Dropbox** app opens and asks if access for **Sophos Mobile Encryption** should be granted.

After access is granted, the list of files in the **Dropbox** account is shown.

4.3 File list views

File lists are updated automatically:

- When you change to a subfolder of the current folder, up-to-date information provided by the cloud server is shown.
- When you return to the parent folder of the current folder, the original information is shown.

- If a **Dropbox** folder was shown when the app was sent to the background and you resume it, the file list is updated with the current information from the cloud.

4.4 View a file

When browsing Dropbox in the file list view, the listed files are not yet on the device. You have to download them from Dropbox before you can view them.

1. Tap a file entry in the file list view to start the download of the selected file. A progress bar shows the download status.
 - If you tap the **X** button at the right-hand side of a file that is currently downloaded, the download is canceled.
 - If you tap a different file while a download of a file is in progress, the download is canceled and the download of the other file you selected is started.
 - If you tap a folder or navigate back, the currently running download is canceled.
2. If the file is encrypted, the **Encryption** app asks you for a passphrase. Enter the passphrase that was used in SafeGuard Enterprise to create the local key for encrypting the file. If you enter a wrong passphrase, a delay of three seconds is imposed before you can retry to enter the passphrase.
3. Tap the **Decrypt** button (checkmark at the right-hand side of the action bar) or the **Done** key on the virtual keyboard.
4. The plain file is forwarded to the associated viewer app. Note that some viewer apps offer editing of documents. As Sophos Mobile Encryption is intended for reading documents only, such changes are lost, they will not be forwarded to the (encrypted) original file.

Note: You can cancel an ongoing decryption process by tapping the **X** button or the left button in the title bar, switching back to the file list. When you cancel decryption, the partially written plain file is deleted.

4.5 Grace period

For your convenience **Sophos Mobile Encryption** remembers an encrypted version of the last successfully used passphrase for a grace period of 10 minutes. When you open the same or a different encrypted file within this period, **Sophos Mobile Encryption** automatically tries to decrypt the file with the remembered passphrase:

- If decryption is successful, the file is opened immediately.
- If the last passphrase does not work, you are prompted to enter the correct passphrase.
- The grace period of 10 minutes restarts when a passphrase is re-used successfully.
- The passphrase is cleared when a re-use attempt fails.

5 Egnyte

To view encrypted files in **Egnyte** on an Android device, files in the cloud storage have to be encrypted on a Windows endpoint that runs SafeGuard Cloud Storage first.

To enable an endpoint to encrypt files in **Egnyte**, it needs a **policy of type Cloud Storage** that allows you to encrypt files in **Egnyte**.

Sophos Mobile Encryption then allows you to view the encrypted files stored in **Egnyte** on an Android device.

5.1 Configure Egnyte

The configuration dialog is displayed, if you tap **Egnyte** in the **Home** view and **Egnyte** has not been configured yet.

Tap the **Link/unlink** icon on the right hand side of the **Egnyte** list entry to link or unlink an **Egnyte** account with Sophos Mobile Encryption.

- **If an Egnyte account has already been linked**, the account info and the **Unlink** icon to unlink the account are displayed. Tap the button to unlink the account.
- **If no Egnyte account is linked**, tap the **Link** icon to trigger the linking of an **Egnyte** account.

5.2 Link an Egnyte account to the app

When you enter the URL and tap the **Link with Egnyte** button in the **Egnyte** configuration dialog you have to provide user name and password. Afterwards the connection to the **Egnyte** server will be established.

After access is granted, the new link state is displayed. Tap the **Done** button to change to the file list view.

6 Media Center

To view encrypted files in **Media Center** on an Android device, files in the cloud storage have to be encrypted on a Windows endpoint that runs SafeGuard Cloud Storage first.

To enable an endpoint to encrypt files in **Media Center**, it needs a **policy of type Cloud Storage** that allows you to encrypt files in **Media Center**.

Sophos Mobile Encryption then allows you to view the encrypted files stored in **Media Center** on an Android device.

6.1 Configure Media Center

The configuration dialog is displayed, if you tap **Media Center** in the **Home** view and **Media Center** has not been configured yet.

Tap the **Link/unlink** icon on the right hand side of the **Media Center** list entry to link or unlink a **Media Center** account with Sophos Mobile Encryption.

- **If a Media Center account has already been linked**, the account info and the **Unlink** icon to unlink the account are displayed. Tap the button to unlink the account.
- **If no Media Center account is linked**, tap the **Link** icon to trigger the linking of an **Media Center** account.

6.2 Link a Media Center account to the app

When you enter user name and password and tap the **Link with Media Center** button in the **Media Center** configuration dialog the connection to the **Media Center** server will be established.

After access is granted, the new link state is displayed. Tap the **Done** button to change to the file list view.

7 Google Drive

To view encrypted files in **Google Drive** on an Android device, files in the cloud storage have to be encrypted on a Windows endpoint that runs SafeGuard Cloud Storage first.

To enable an endpoint to encrypt files in **Google Drive**, it needs a **policy of type Cloud Storage** that allows you to encrypt files in **Google Drive**.

Sophos Mobile Encryption then allows you to view the encrypted files stored in **Google Drive** on an Android device.

7.1 Configure Google Drive

The configuration dialog is displayed, if you tap **Google Drive** in the **Home** view and **Google Drive** has not been configured yet.

Tap the **Link/unlink** icon on the right hand side of the **Google Drive** list entry to link or unlink a **Google Drive** account with Sophos Mobile Encryption.

- **If a Google Drive account has already been linked**, the account info and the **Unlink** icon to unlink the account are displayed. Tap the button to unlink the account.
- **If no Google Drive account is linked**, tap the **Link** icon to trigger the linking of an **Google Drive** account.

7.2 Link a Google Drive account to the app

After tapping the **Link** icon you can choose an existing Google Drive account or add a new one. If you tap on a **Google Drive** account, the connection to the **Google Drive** server will be established.

After access is granted, the new link state is displayed. Tap the **Done** button to change to the file list view.

8 Link an account using WebDAV

A configuration dialog is displayed when you tap on **WebDAV** in the **Home** view. Here you can enter the **Server URL** of any cloud storage provider that supports access using the WebDAV protocol.

To link an account enter **Server URL**, **Username** and **Password** and click Link with **WebDAV**.

9 Favorites

Favorites are local copies of files in cloud storage that can be read without a connection to the cloud. By marking files as **Favorites** you can download them for offline reading.

Note: The list of **Favorites** is emptied when you unlink an account.

9.1 Marking files as Favorites

- Entries in the file lists for **Dropbox** and **Favorites** show star-shaped **Favorite** icon at the right-hand side of the entry. An empty star icon indicates that the file is not on the **Favorites** list.
- If you tap on the empty star icon in **Dropbox**, the file is added to the **Favorites** list. Sophos Mobile Encryption saves a local copy of the file. The empty star changes to a full star. The full star icon indicates that the file is on the **Favorites** list.
- If you tap on a full star icon in **Favorites** or **Dropbox**, the file is removed from the **Favorites** list. Sophos Mobile Encryption deletes the local copy of the file. The full star changes to an empty star.

9.2 Reading files offline

Tap **Favorites** in the **Home** view to display the list of files marked as **Favorites**.

Note: As **Favorites** with identical names may originate from different folders in cloud storage, there may be multiple entries with identical names in the list.

You can read the files in the list without a connection to the cloud.

All files in **Favorites** have a full star icon. If you tap it, the file is removed from **Favorites**. You can only add files to **Favorites** from one of the cloud storage provider views.

9.3 Updating local copies

When you open a file from **Favorites**, the local copy of the file is displayed. If a newer version of the file exists in the cloud and you want to have your local copy updated, you can either open the file from a storage provider view or tap the synchronize button in the action bar in the **Favorites** view.

When you open a file from a cloud storage provider view, the latest version is shown:

- If there is a local copy in **Favorites** that is up-to-date, the local copy is opened.
- If there is a local copy in **Favorites** that is not yet up-to-date, the latest version is downloaded from the cloud, copied to **Favorites** and then opened.

The **Favorites** view offers a synchronize icon for retrieving the current versions for all files. When you tap the icon in the action bar, the overlay icons for all items in the list change to gray. This indicates that they are checked for newer versions. Whenever a file has been checked and a newer version has been downloaded or the file has been found to be up-to-date, the color of the overlay icon changes back to pink. Synchronization is done in the background. You can leave the view while synchronization continues. Files that are marked as **Favorites**, but are no longer stored in the cloud, are removed from the **Favorites** view.

Synchronization ends when the app is closed and does **NOT** continue after a restart.

10 Technical support

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

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/en-us/support.aspx>
- Download the product documentation at <http://www.sophos.com/en-us/support/documentation.aspx>
- Send an email to support@sophos.com, including your Sophos software version number (as shown in the about screen that can be opened from the menu) and Android device information.

11 Copyright

Copyright © 2010 - 2013 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

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.