Cybersecurity
made
simple.

Sophos Secure Workspace

help

product version: 9.6

Contents

1 Introduction

Sophos Secure Workspace allows you to store files on mobile devices or in the cloud, even across multiple storage providers, and ensure the privacy of your sensitive data. In a corporate environment, you may want to access documents and intranet pages and store files, bookmarks, and credentials in a safe place.

Sophos Secure Workspace enables you to:

- View documents stored locally or in the cloud. See View documents (page 7).
- Manage documents stored locally or in the cloud. See Manage documents (page 8).
- Annotate PDF documents and fill out PDF forms. See Edit PDF documents (page 11).
- Take notes. See Take notes (page 12).
- Take photos. See Take photos (page 13).
- Manage archive files in ZIP and 7z format. See Manage archive files (page 15).
- Ensure the privacy of your data by encrypting documents. See Ensure the privacy of your data (page 14).
- Securely share documents between users. See Share files between users (page 15).
- Access the content of password protected files that you received from SafeGuard Enterprise users. See Password protect files (page 21).
- Store and manage all your passwords in the integrated Password Safe. See Manage passwords (page 29).

On iOS, you can get a menu of quick actions when you touch and hold the Sophos icon. On a 3D Touch device, you can press briefly on the icon to see the menu.

If you are using other Sophos products, you have additional options.

Customers who have **Sophos Mobile** can:

- Create or edit Microsoft Word, Excel or PowerPoint files using the integrated Polaris Office. See Edit Office documents (page 10).
- Securely access corporate intranet pages and other allowed pages. See Access the corporate intranet (page 18).
- Securely view documents from your company. See View work documents (page 20).
- Create and share password protected files that are wrapped in an HTML5 format. See Password protect files (page 21).
- Manage Sophos Secure Workspace settings and cloud storage credentials.

Customers who have **SafeGuard Enterprise** on Windows or macOS can:

- Securely share documents between mobile devices, notebooks, and desktop computers. See Share files between devices (page 17).
- Use the keys from their SafeGuard keyring. See Manage keys (page 25).
- Display their recovery keys for BitLocker and FileVault disk encryption. See Display recovery keys (page 28).

Sophos Secure Workspace shares information with other Sophos apps via the **Sophos container**:

- The app password is used by both Sophos Secure Email and Sophos Secure Workspace.

- Sophos container actions (lock, unlock, reset password, unenroll) are applied to all Sophos container apps.
- Data and files can be securely shared between Sophos container apps.

2 Local Storage

The **Local Storage** page shows files on your device.

On Android, Local Storage contains the files in the device storage, excluding the SD card.

On iOS, apps can only access files within their own container. Therefore, Local Storage contains the files you have created or imported into Sophos Secure Workspace.

Copy files to a computer

Connect your device to a Windows computer or Mac to copy files.

(On Android) Select the **Transfer files** USB mode. Windows Explorer shows the device storage under **This PC**.

(On iOS) In iTunes, use the **File Sharing** list for Sophos Secure Workspace.

3 Secure Storage

Secure Storage is a secure container on your device only Sophos Secure Workspace can access.

When you save files in Secure Storage they are encrypted with a device key, unless they're already encrypted.

When you move files out of Secure Storage, they are unencrypted, unless they were originally encrypted.

Sophos Secure Workspace automatically deletes files in Secure Storage when any of the following happen:

- You uninstall the Sophos Secure Workspace app.
- The Sophos Secure Workspace app is no longer managed by Sophos Mobile.
- (On Android) You delete the app data.

4 Connect cloud storage

To connect your cloud storage account to Sophos Secure Workspace:

1. On the **Home** page, do one of the following:
   - (On Android) Tap **+**.
   - (On iOS) Tap the **Add cloud storage** ☁ icon.
2. Select a storage provider.
3. Enter your credentials.

Sophos Secure Workspace creates a tile on the **Home** page for each storage provider you connect.

5 Favorites

You can collect files in the **Favorites** list to easily access them. Favorites are available even when the device is offline.

To add a file to favorites:

- (Android) Select **Star** ★ next to the file name.
- (iOS) Select the file and then **Star** ★.

You can also select a folder to add all files in that folder, including its subfolders, to favorites.

In Android, you can add favorites to the Home screen.

6 View documents

To view a document, navigate to its storage location and tap it. If the file is encrypted with a key that isn’t available in the Sophos Secure Workspace keyring, you must enter the passphrase for the key. Encrypted files are marked with a lock icon.

For the file types you can view and edit with Sophos Secure Workspace, see Supported providers and formats (page 37).

7 Manage documents

You can perform various operations on your documents, for example encrypt them, move them to a cloud storage, or share them with other apps.

File operations

You can copy, move, rename, and delete files and folders.

Restrictions:

- You can’t copy or move files or folders from one cloud storage to another or to device storage.
- You can only rename a single file or folder at a time.
- Google Drive doesn’t support copying or moving folders.
- (iOS) You can’t create folders in Local Storage.

View file properties

You can view file properties like the file size or encryption key details.

If Sophos Secure Workspace is managed by Sophos Mobile, you can also view information about usage restrictions defined by your organization.

- (Android) Select a file and then **File details** from the **File operations** 🖹 menu.
- (iOS) Select a file and then **File Details** from the **More** ◦◦◦ menu.

Move files to cloud storage

You can move a file from device storage to cloud storage. The file is deleted on the device.

Note
We recommend that you encrypt files before you move them to a cloud storage.

Add files to favorites

You can collect files in the **Favorites** list to easily access them. Favorites are available even when the device is offline.

To add a file to favorites:

- (Android) Select **Star** ★ next to the file name.
- (iOS) Select the file and then **Star** ★.

You can also select a folder to add all files in that folder, including its subfolders, to favorites.

In Android, you can add favorites to the Home screen.

Encrypt and decrypt files

You can encrypt files, or decrypt them if they’re encrypted.

To encrypt files:

- (Android) Select the files and then **Encrypt** 🔑. Depending on your display size, you might have to select **More** ⋮ first.
- (iOS) Select the files and then **Encrypt** from the **More** ◦◦◦ menu.

You can also select a folder to encrypt all files in that folder, including its subfolders.

To decrypt a file:

- (Android) Select the file and then **Decrypt** ⚿. Depending on your display size, you might have to select **More** ⋮ first.
- (iOS) Tap the file, enter the passphrase, and then select **Decrypt**.

Use files from other apps in Sophos Secure Workspace

You can use files from other apps in Sophos Secure Workspace.

- (Android) Select **+** and then **Import existing**.
- (iOS) Select **Import Existing** from the **More** ◦◦◦ menu.

If supported, you can also select files in the source app and use **Open with** (Android) or **Open In** (iOS) to share them with Sophos Secure Workspace.

Note

- (Android) When you import a mixture of encrypted and unencrypted files you can’t choose to encrypt the unencrypted files. The files are imported with their current encryption status.
- (iOS) You can use drag and drop to move files between Sophos Secure Workspace and other apps.
- (iOS) The **Save to Workspace** and **View with Workspace** activities are turned off by default. To turn them on, tap **More** in the **Share** list.

Use files from Sophos Secure Workspace in other apps

You can use files from Sophos Secure Workspace in other apps. To do this, select the file and share as usual.

(Android) Some apps let you select documents from Sophos Secure Workspace in their file selection dialogs. For example in Gmail, you can select document from Sophos Secure Workspace as email attachment.

Note

If Sophos Secure Workspace is managed by Sophos Mobile, your organization may have forbidden sharing for certain storage providers.

8 Edit Office documents

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

Sophos Secure Workspace includes a Polaris Office library that lets you create or edit Microsoft Word, Excel and PowerPoint files.

Create a Microsoft Office document

To create a Microsoft Office document:

1. Navigate to the storage location where you want to create the file and then tap **+**.
2. Select **Word**, **Excel** or **PowerPoint** to open the embedded Polaris Office.

View or edit Microsoft Office documents

To view or edit an existing Microsoft Office document:

1. Navigate to the file and then tap it to open it in the embedded Polaris Office.
2. Use the Polaris Office menu to switch between viewing and editing mode.

Note
When you edit an encrypted Office document, it will automatically be encrypted again when you save it.

Restrictions

Your organization can configure sharing restrictions for storage providers. These have the following effects in the embedded Polaris Office:

- If your organization has denied the sharing of files, you cannot use **Export** in Polaris Office.
- If your organization has denied clipboard operations, you can still use the clipboard within Polaris Office, but cannot paste the clipboard content into another app.

9 Edit PDF documents

Note

This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

Mobile devices can be used for reviewing documents or for entering the small amounts of data needed for PDF forms.

Sophos Secure Workspace provides an integrated viewer and editor for PDF documents.

To edit a PDF or fill in a PDF form:

1. Open the PDF file.
    - Tap the **Add Annotation** button to annotate a document. You can highlight text or use tools like notes, text, drawing, line, rectangle or arrow.
    - Tap a field in a PDF form and fill it out.
2. Save your changes.

    If the file was encrypted, it is automatically encrypted again when you save it.

10 Take notes

Sophos Secure Workspace lets you create a quick note. You can encrypt the note to ensure privacy.

Android:

1. Navigate to the storage location where you want to create the file.
2. Select **+** and then **Text**.
3. Enter your note.
4. When done, select **Save**.
5. Enter a file name and select an encryption key.

iOS:

6. Navigate to the storage location where you want to create the file.
7. Select **Create > Text File** from the **More** ◦◦◦ menu.
8. Enter your note.
9. When done, select **Done**.
10. Enter a file name and select an encryption key.

Note
If Sophos Secure Workspace is managed by Sophos Mobile, you can also create or edit Microsoft Office files. See Edit Office documents (page 10).

11 Take photos

Sophos Secure Workspace lets you take photos and store them securely. The photos are not available to other apps on your device unless you explicitly share them.

Android:

1. Navigate to the storage location where you want to create the photo.
2. Select **+** and then **Photo**.
3. Take the photo.
4. Enter a file name and select an encryption key.

iOS:

5. Navigate to the storage location where you want to create the photo.
6. Select **Create > Photo** from the **More** ◦◦◦ menu.
7. Take the photo.
8. Enter a file name and select an encryption key.

12 Ensure the privacy of your data

Your data has value and should be protected. We recommend that you always encrypt your sensitive data, whether you store it locally on your device or in the cloud.

Encryption is a method of scrambling data in a format that is only readable by authorized users. Although encryption won't stop data loss or theft, it keeps your data safe by making it unreadable and unusable to an attacker. When you encrypt a file, it is secured by a key so that only a person that knows the key can access the file.

For a quick overview of how encryption works in Sophos Secure Workspace, see Security information (page 36).

Encrypt files

Encrypting files is easy with Sophos Secure Workspace.

When a new file is created by this app or imported from another app, you can encrypt it.

To encrypt an existing file:

1. Select the file in the list and choose the **Encrypt** option.
2. Choose the encryption key to be used. If there is no key yet, you can create one now.
3. Tap **OK**. The selected file is encrypted. If the selection contains folders, all files within folders will be encrypted as well.

Note
If you encrypt a file that is already encrypted, it will be re-encrypted with the new key. If a passphrase is required for the old encryption key and the key is not available in your keyring, you are asked to enter the passphrase.

Note
If Sophos Secure Workspace is managed by Sophos Mobile, you can only encrypt files with keys from your corporate keyring, not with local keys. For information on using your corporate keyring, see Manage keys (page 25).

Decrypt files

To decrypt existing files, select them in the file list and choose the **Decrypt** option.

Sophos Secure Workspace asks you to enter the passphrase to access the data. You are not asked for passphrases of keys that are available in your keyring.

Note
If Sophos Secure Workspace is managed by Sophos Mobile, you cannot decrypt files.

13 Share files between users

Encryption keys in Sophos Secure Workspace are derived from passphrases.

Do not create a new encryption key for every file but think about how you want to organize access to your content.

If you have a group of files that should be shared with other persons:

- Encrypt all these files with the same encryption key.
- Tell the other users the passphrase for the key.
- If another user, with access to the same file (for example using shared cloud storage), opens the file from their device and the key is not yet in their keyring, Sophos Secure Workspace asks for the passphrase. If the user enters the correct passphrase, the encryption key is added to their keyring. This is why you only need to distribute the passphrases, not the encryption keys.

Note
Two encryption keys created from the same passphrase will be different. This is because some random data is added during key creation to improve security. Tell recipients of your encrypted files not to create encryption keys before receiving files but to wait until they are asked for the passphrase for a document.

Note
If Sophos Secure Workspace is managed by Sophos Mobile, you can share files without the need to distribute a passphrase if both you and the recipients have the encryption key in the corporate keyring.

13.1 Manage archive files

With Sophos Secure Workspace you can manage archive files in ZIP and 7z format.

View the content of an archive file

You can browse archive files in ZIP or 7z format and view the content of included files without extracting them.

- To browse a ZIP or 7z archive file, navigate to the file and then tap it. If the archive file is password protected, you must enter the password.
- To view the content of a file within the archive file, navigate to that file and then tap it. If Sophos Secure Workspace supports the file format, the file opens in the embedded viewer.

Extract an archive file

To extract all files from a ZIP or 7z archive file:

- Select the archive file and then tap **Extract** in the menu.
- Alternatively, open the archive file and then tap **Extract all** in the menu.

Extract a single file from an archive file

To extract a single file from a ZIP or 7z archive file:

1. Open the archive file.
2. Navigate to the file you want to extract and select it.
3. Tap **Extract selected** in the menu.

Create a ZIP archive file

You can compress selected files and store them in a new ZIP archive file, optionally with password-based ZIP encryption.

You can also encrypt the archive file with an encryption key from the Sophos Secure Workspace keyring.

To create a ZIP archive file:

1. Navigate to the folder that contains the files you want to store in an archive file.
2. Select one or more files and then tap **Compress** in the menu.

   You can't select files from **Favorites**, **Work documents** or **Recently opened**.

Note
If Sophos Secure Workspace is managed by Sophos Mobile and sharing of files is forbidden for a storage provider, you can't store such files in an archive file.

14 Share files between devices

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

Files encrypted by Sophos Secure Workspace can be read and modified by Sophos SafeGuard Enterprise and vice versa.

Sophos SafeGuard Enterprise is a business-level solution for disk and file encryption. It is available for notebooks or desktop workstations using Windows or macOS. The Cloud Storage and File Encryption modules of SafeGuard Enterprise offer transparent encryption of data in the cloud.

If you share a file with a device that does not have the encryption key in the keyring, you must enter the passphrase to open the file.

15 Access the corporate intranet

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

Work browser

The work browser allows you to securely access corporate intranet pages and other allowed pages, as defined by a Sophos Mobile policy. Your organization can define a set of work bookmarks that can be accessed from the work browser. You can then add any sub-page to your personal bookmarks.

The work browser supports tabbed browsing, i.e. you can work with multiple web pages at the same time. When you start the work browser, all tabs opened in the previous session will be re-opened.

- To start the work browser, tap **Work browser** on the **Home** page.
- To access bookmark settings and related functions, tap **More** ⋮ in the top right corner of the screen (Android) or use the toolbar (iOS).

Bookmarks

- The **Work bookmarks** page contains bookmarks added by your organization.
- The **Personal Bookmarks** page contains bookmarks added by you. Tap the **Star** ★ icon to bookmark the current web page.
- The **History** page contains a chronological list of the web pages you've visited. To remove a single item from the list, swipe left or right. To clear the list, tap **Clear history** (Android) or the **Delete** 🗑 icon (iOS).

Credentials

You can manage your credentials for specific websites if your organization has defined the policy to allow you do so.

When you enter your user name and password, Sophos Secure Workspace prompts you to save your credentials. Tap **OK** to save your credentials in the credentials manager. They are available the next time you visit this page.

The **Credentials** page contains the credentials you've saved. To delete an entry, swipe left or right.

Downloads

Most links in web pages are links to other pages. Sometimes they are links to documents or lists of files that can be managed via a web interface, for example, SharePoint. When you tap a link that references a document, the work browser checks for the permissions defined for the domain in question.

Your organization can define the following permissions:

- You are allowed to view the file.
- You are allowed to download and view the file.
- You are allowed to download and open the file in a different application.

When you download a file, it is saved in **Secure Storage**. If the file is not encrypted, the local copy is encrypted with a device key.

16 View work documents

Note

This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

Sophos Mobile includes its own file distribution server which appears as an additional storage provider called **Work documents**.

You can use the work documents feature as follows:

- Your organization can upload files on the Sophos Mobile web portal.
- Files are read-only for the users: content can be viewed, but not modified.
- Your organization can define groups of users and restrict visibility of files to certain groups.
- Your organization can define data leakage rules for each file separately. See Corporate settings (page 35).

You are informed when new or updated documents are available in **Work documents**. Each new or updated file is marked as new.

If you mark files or folders of the **Work documents** storage provider as favorites, Sophos Secure Workspace ensures that the offline copies are encrypted, using an encryption key that is restricted to the device.

If your organization wants to encrypt files for distribution with Sophos Mobile, this can either be done on a mobile device by encrypting files in the **Local Storage** view of Sophos Secure Workspace or (more easily) using Sophos SafeGuard Enterprise.

17 Password protect files

In addition to the standard (key-based) file encryption, Sophos Secure Workspace also lets you create password protected files that are wrapped in an HTML5 format, so it doesn’t require the recipients to install any software. All they need is the password and a web browser (in Windows or macOS) or the Sophos Secure Workspace app (in Android or iOS) to access the encrypted content.

For example, this is useful when you want to share files with recipients outside your organization.

View or edit password protected files

You can view password protected files that have been created with Sophos Secure Workspace (in Android or iOS) or with SafeGuard Enterprise (in Windows or macOS).

Tap the HTML container and enter the correct password to access the files inside.

- If the container contains only one file and viewing is supported for the file type, the file is opened for viewing. You can switch from viewing mode to editing mode and make changes if editing is supported for the file type. When you save the changed file, it is stored as a new file outside the HTML container.
- If the container contains multiple files, select a storage location to store the files outside the HTML container. Select **Encrypt** to encrypt the files in their new location. After you have stored the files, you can view and edit them.

Create a password protected file

Note
The creation of password protected files is only available if Sophos Secure Workspace is managed by Sophos Mobile.

1. Select the file you want to password protect and then do one of the following:
   - (Android) Select **Share password protected** from the **More** ⋮ menu.
   - (iOS) Select **Share Password Protected** from the **Share** 📤 menu.
2. Enter a password.
3. Choose the app with which you will transfer the password protected file, for example your email app.

Note
If the file you want to share is encrypted, Sophos Secure Workspace will decrypt it, if possible, and then password protect the unencrypted file.

18 Check web links in documents

Sophos Secure Workspace protects you from browsing web sites with malicious, undesirable or illegal content.

- When you tap a link in an Microsoft Office or PDF document, Sophos Secure Workspace checks the URL and displays threat information about the target web page.
- Access to web pages is not blocked automatically. After reading the threat information, you can decide to cancel the operation or open the web page.
- The web pages are opened in the work browser, if available, or in your default browser app otherwise.

19 App password

App password

You can specify a password to protect Sophos Secure Workspace from unauthorized access. If you activate the setting, you are prompted to enter and confirm the password the next time you start the app. The app password has to be entered each time you start Sophos Secure Workspace.

Note that Sophos Secure Workspace uses the same password as Sophos Secure Email. Any changes to the password thus apply to both apps. When you are logged in to one of the apps, you do not have to enter your credentials for the other one (single sign-on). The password and configurations from your organization are stored in the Sophos container, which protects data used by Sophos apps on your device.

You can use fingerprint authentication to log in to Sophos Secure Workspace. However, you have to define an app password as a fall-back in case your fingerprint cannot be read.

Note
In Android, fingerprint authentication is only available if Sophos Secure Workspace is managed by Sophos Mobile and if the device supports it.

Recovery password

Sophos Secure Workspace can generate a recovery password for your app password and send it to you by email. If you forget the app password, you will need this recovery password in order to create a new app password. If you forget the app password but do not have a recovery password, you cannot use the app any more without deleting and re-installing it. When you delete the app, you lose all your local documents kept by Sophos Secure Workspace and the keys stored in your keyring.

CAUTION
We strongly recommend creating a recovery password. If you forget the app password, you can only reset it using the recovery password.

Note
If Sophos Secure Workspace is managed by Sophos Mobile, a recovery password is not required. You can reset the app password from the Sophos Mobile Self Service Portal.

Grace period

For convenience, you can specify a grace period, i.e. a time frame within which you do not have to enter the app password again when you start the app. During the grace period, you can start Sophos Secure Workspace (as well as Sophos Secure Email) without having to enter the password again. The grace period is only valid while the app is in memory. When the app is loaded by the system, you always have to enter the app password.

When the device is locked, Sophos Secure Workspace is locked as well regardless of the grace period setting.

Set the app password

You set the app password, the recovery password and the grace period on the **Settings** view.

Change the app password

You can change your app password in the **Login** view that is displayed when you start Sophos Secure Workspace. When changing your app password, you can request a new recovery password. If you do not request a new one, the old recovery password remains valid for the new app password.

20 Manage keys

Sophos Secure Workspace collects all your encryption keys in a keyring. You can see them by tapping **Encryption keys** in the menu.

Keyring removal

- The Sophos Secure Workspace keyring is removed from the device when the app is uninstalled.
- Encrypted files in the cloud or on storage cards in Android devices remain encrypted. When the keyring is removed, you are no longer able to access these files.

Loss of encryption keys

- If you lose the encryption key, you can still access encrypted files if you remember the passphrase.
- Sophos Secure Workspace asks you to enter the passphrase and adds the key to the keyring again.

CAUTION
If you lose the encryption key and you can’t remember the passphrase, you can’t access your content. If there were a backdoor for reading the content without having the key or knowing the passphrase, this could be used by attackers as well.

Corporate keyring

If Sophos Secure Workspace is managed by Sophos Mobile, your organization can activate a corporate keyring sync with Sophos SafeGuard. This makes the keys from your SafeGuard keyring available in the Sophos Secure Workspace keyring.

This means that:

- If there are local keys in your keyring when corporate keyring sync is activated, you can continue to use them.
- After corporate keyring sync is activated, you can’t create new local keys.
- If configured by your organization, your corporate keys are removed from the device when the Sophos container is locked, for example when your device violates compliance rules.

Share encryption keys by using QR codes

You can easily share local keys by using QR codes. For example, you can attach the key to an email and the recipients can add the key to their keyring by scanning the QR code.

We recommend that you protect the exported key with a passphrase. When recipients add the key to their keyring they have to enter the passphrase.

You cannot export keys from the corporate keyring. You can export local keys when corporate keyring sync is activated, if your organization's policy allows this.

To export a local key:

1. Select the key you want to export and then do one of the following:
    - (Android) Select **Share** <.
    - (iOS) Select **Export**.
2. Enter a passphrase and select **Protect** (Android) or **Share with passphrase** (iOS).
3. When the QR code is displayed, select **Share** (Android) or **Open In** (iOS).
4. Attach the key to an email or select a storage location.

To import a key:

1. Select **Encryption keys** in the menu and then do one of the following:
    - (Android) Select the QR code icon and scan the key's QR code.
    - (iOS) Select **+** and then **Import key from QR code** and scan the key's QR code.
2. If required, enter the passphrase.
3. The key is added to your keyring.

21 Display certificates

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

You can display these types of certificates:

- The SMC client certificate.
- The client certificate that has been issued through SCEP, if configured in the Sophos container policy.
- All client and root certificates that have been transferred to the device as part of the Sophos container policy.

To display certificates:

- Tap **Settings** in the menu to open the **Settings** view. In the **Certificates** section, the certificates are displayed with subject and purpose information.
- Tap a certificate to display additional details.

22 Display recovery keys

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

If you are locked out from your computer on which BitLocker Drive Encryption (on Windows) or FileVault full disk encryption (on macOS) is turned on, you must enter a recovery key to unlock the computer and access your data.

Your organization can make the recovery keys for your computers available to you in Sophos Secure Workspace.

To display the recovery key for a computer:

- Tap **Recovery keys** in the menu to display a list of computers that are assigned to you. For Windows computers the list contains individual entries for each disk partition.
- Tap a list entry to display the recovery key for that computer or disk partition.
- To unlock your computer, follow the instructions that are displayed on the BitLocker (on Windows) or FileVault (on macOS) screen on your computer.

23 Manage passwords

Sophos Secure Workspace lets you manage KeePass Password Safe files.

Features

- Create a new Password Safe file
- Edit the content of the Password Safe file
- Copy passwords or other data to the clipboard to use it in other apps
- Edit an existing KeePass Password Safe file that is located in a cloud storage

Supported formats and encryption standards

- Sophos Secure Workspace supports version 3 of KDBX file format. It can open files that use one of the native KeePass encryption algorithms (AES, ChaCha20).
- New Password Safe files are created with KDBX file format version 3 format using AES encryption.

23.1 Create Password Safe file

1. Navigate to the storage location where you want to create a Password Safe file.
2. Tap **+** and then tap **Password Safe**.
3. Create a master password for the Password Safe file. This password is required to open the Password Safe file.

   Warning
   If you forget the master password, there is no way to access your passwords and other Password Safe data.

4. Optional: For Android, select to use a key file.

   Using a key file in addition to the master password increases the security of your Password Safe file. A key file can be any file you choose or you can create one. It must be available when you open your Password Safe file.

   Select **Use key file** and tap **+** to create a file, or select an existing file. Don’t store your key file together with your Password Safe file.

   Warning
   You must back up your key file. Without it there is no way to open your Password Safe file.

   For iOS, you can configure a key file in the settings of your Password Safe file. Tap **Change Master Password** and turn on **Use Key File**.
5. For iOS, enter the required entries to the Password Safe file. You can organize your entries in groups or sub-groups.

   For Android, you save the new Password Safe file first and then enter your password entries.

6. Tap **Create**, enter a name and location and tap **Store**.
7. Optional: Select to encrypt the Password Safe file.

   All Password Safe files are encrypted with KeePass file encryption. When you select the encryption option in the **Save file** dialog, Sophos Secure Workspace adds an additional encryption layer on top of the KeePass encryption.

A KDBX file is created in the specified location.

23.2 Create Password Safe entry

To add an entry or entry group to a Password Safe file:

1. Open the Password Safe file and then tap **+**.
2. Select the type of entry you want to create:
   - **Account** creates an entry with predefined fields suitable for web accounts and similar items.
   - **Credit card** creates an entry with predefined fields suitable for credit cards and similar items.
   - **Note** creates an entry to store notes. Only available on iOS.
   - **Group** creates a folder within the Password Safe file to organize your entries.
3. Enter your data into the fields of the entry.
4. Optional: For Android, tap the icon next to the **Title** field to select a different one.
5. Optional: Add custom fields to the entry.
   - (On Android) Tap **Add field** and then add a field name and a value.
   - (On iOS) Tap **+** and then select the type of field that you want to add.

   When you turn on **Protected** for a custom field, its value is hidden unless you tap the **Eye** 👁 icon next to the field. Also, protected fields are excluded from search results.
6. When done, save the entry:
   - (On Android) Tap **More** 💾.
   - (On iOS) Tap **Done**.

You can easily use the password data to log in on a web page or in an app. See Use password data to log in (page 31).

Note

On iOS, you can attach files to a Password Safe entry. However, you might experience performance problems if you attach large files or a large number of files. To securely store such files, we recommend you encrypt them with Sophos Secure Workspace.

23.3 Generate passwords

Sophos Secure Workspace can auto-generate passwords for you.

1. In the Password Safe file, open the entry for which you want to generate a password.
2. Switch to edit mode:
   - (On Android) Tap **Edit** ✎.
   - (On iOS) Tap **Edit**.

3. Open the password generator:
   - (On Android) Tap **+** next to the password field.
   - (On iOS) Tap the **Cogwheel** ⚙ icon.
4. Define the password length and the types of characters that must be included in the password.
5. Generate a password based on your specification:
   - (On Android) Tap **Generate password**.
   - (On iOS) Tap **Refresh** ↻.
6. When you are happy with the generated password, close the password generator.

   The password is updated with the generated value.
7. Save the entry.

23.4 Use password data to log in

- To copy a field value to the clipboard, tap the required field.
- To display the value of protected fields, tap the **Eye** 👁 icon next to the protected field.
- To open a URL in the web browser:
  - (On Android) Tap the URL. To copy the URL to the clipboard instead, tap and hold it.
  - (On iOS) Tap the **Globe** 🌐 icon next to the **URL** field.

Tip

In Android, Sophos Secure Workspace adds a notification to the Android notification area when you open an entry. From that notification, you can copy the user name and password values to the clipboard.

23.5 Manage Password Safe entries

1. Tap and hold an entry to switch to select mode.
2. Optional: Select more entries for which you want to perform the same action.
3. Tap an icon to perform the required action:
   - **Edit** ✏ - Edit the content of the entry. Only available when a single entry is selected.
   - **Cut** ⬚ - Move the selected entries to another group in the Password Safe file.
   - **Copy** ⧉ - Copy the selected entries to another group in the Password Safe file.
   - **Delete** 🗑 - Move the selected entries to the special **Recycle bin** group. To delete entries permanently, use **Delete** 🗑 on entries in the **Recycle bin** group.
   - To paste an entry you've cut or copied, navigate to the target location and then tap **Clipboard** 📋.

23.6 Search Password Safe entries

You can search for entry names and for values of entry fields. In Android, you can also search for group names.

1. (On iOS) If you don’t want to search the whole Password Safe file, navigate to a group or subgroup. All items within that group are searched recursively.
2. Switch to search mode:
   - (On Android) Tap **Search** 🔍.
   - (On iOS) Swipe down in the Password Safe view.
3. Enter a search string. The list of results is updated as you type.

> **Note**
> Password fields and fields that you configured as **Protected** are excluded from the search results.

23.7 Manage master passwords

When you open a Password Safe file in Sophos Secure Workspace that is secured with a master password, select **Remember password** to store the master password in the Sophos Secure Workspace keyring. The next time you open that Password Safe file you are not asked for the master password.

To view the master passwords stored in the Sophos Secure Workspace keyring, tap **Passwords** in the menu.

To make Sophos Secure Workspace forget a master password, delete it from the keyring.

24 Settings

Setting	Description
Enable keyring	Turn on this option to store encryption keys in a keyring. You don’t have to enter a passphrase for keys stored in the keyring.
Enable app password	Set a password to open the app. We recommend that you also select the option to create a recovery password. You need the recovery password to reset the app password. CAUTION If you have forgotten the app password and don’t have a recovery password, you can’t use the app anymore.
Change app password	Use this option to change the app password.
Grace period	Select the length of time the app remains unlocked when you leave it.
Block screenshots	Turn on this option to block screenshots of the app.
Hide password	Turn on this option to hide passwords you enter in the app. If you turn off this option, characters you enter in password fields are briefly displayed before they are hidden.
Data tracking	Allow Sophos to collect anonymous usage data to improve the app.
Send trace	Tap to send an email with the app’s log file attached. The email address of Sophos Support is inserted by default.
Certificates	Display the certificates managed by Sophos Mobile. See Display certificates (page 27).

Setting	Description
App password	Set a password to open the app. We recommend that you also select the option to create a recovery password. You need the recovery password to reset the app password. CAUTION If you have forgotten the app password and don't have a recovery password, you can't use the app anymore.
Grace period	Select the length of time the app remains unlocked when you leave it.
Touch ID authentication	Turn on this option to allow unlocking the app with your fingerprint.
Hide password characters	Turn on this option to hide passwords you enter in the app. If you turn off this option, characters you enter in password fields are briefly displayed before they are hidden.
Log level	If asked by Sophos Support, select the level of logging information.
Send log files	Tap to send an email with the app's log file attached. The email address of Sophos Support is inserted by default.
Data tracking	Allow Sophos to collect anonymous usage data to improve the app.

25 Corporate settings

Note
This section only applies if Sophos Secure Workspace is managed by Sophos Mobile.

By assigning a Sophos container policy to your device, your organization can configure settings for the Sophos Secure Workspace app and the Sophos Secure Email app.

Your organization can:

- Enforce usage of an app password.
- Define minimum requirements for the app password.
- Define which cloud storage providers are available.
- Configure credentials for WebDAV-based cloud storage access.
- Configure credentials for the Egnyte cloud storage provider (iOS).
- Block screenshots showing the Sophos Secure Workspace app or the work browser (Android only).
- Restrict the app usage:
    - Forbid the creation of favorites.
    - Forbid clipboard operations.
    - Forbid the sharing of unencrypted files.
    - Forbid the sharing of encrypted files.
    - Forbid access for rooted (Android) or jailbroken (iOS) devices.
    - Restrict usage of the app to a specific Wi-Fi connection.
    - Restrict usage of the app to time intervals and days in the week (time fencing).
    - Restrict usage of the app to a list of geographic locations (geo fencing).

26 Security information

Security

Storage of cloud storage credentials and file encryption keys:

- For iOS, the system keychain is used.
- For Android, the system key store is used.

If you have set an app password as described in App password (page 23), the following local data is encrypted:

- Device key (used for Secure Storage, core data, locally stored work documents, work browser downloads)
- Local keys
- SafeGuard encryption keys
- BitLocker and FileVault recovery keys
- Client certificates
- Root certificates
- Container policies
- Connection settings

Warning
We strongly recommend that you create a device lock screen password to improve the security of the key store (Android) or keychain (iOS).

Warning
We strongly discourage rooting (Android) or jailbreaking (iOS) your device as this weakens the security of the key store or keychain.

File encryption and keys

- Sophos Secure Workspace encrypts files using the AES-256 encryption standard. Each file has its own data encryption key (DEK).
- The DEK itself is also encrypted using an AES-256 key encryption key (KEK). The encrypted DEK is stored with the file.
- Sophos Secure Workspace calculates the KEK from a passphrase entered by the user, using the PKCS#5 encryption standard.
- Note that due to the specifics of this method and to improve security, some random data is added, so that creating two KEKs from the same passphrase results in two very different keys.
- The list of KEKs available to a user is called the Sophos Secure Workspace keyring.

27 Supported providers and formats

Supported cloud storage providers

Supported cloud storage solutions are:

- Box
- Dropbox and Dropbox Business
- Egnyte
- Google Drive
- Microsoft OneDrive and OneDrive for Business (also as part of an Office 365 subscription)
- Telekom MagentaCLOUD (formerly Media Center)

Additional cloud storage solutions, when using Sophos Mobile:

- All WebDAV-based cloud storage (for example ownCloud or Strato HiDrive)
- Work documents

Supported file formats

With Sophos Secure Workspace, you can view files of the following types:

- **View and modify:**
  - PDF documents: PDF
  - Text: TXT, TEXT, LOG, ASC, DIFF, CONF, PROPERTIES
  - Microsoft Office (requires Sophos Mobile): DOCX, XLSX, PPTX
  - KeePass Password Safe files: KDBX version 3 with encryption AES or ChaCha20
  - Archive files: ZIP (view, extract, create)
- **View only (with internal viewer):**
  - Images: JPG, JPEG, PNG, GIF (not animated), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Audio (Android): all formats and codecs supported by Android
  - Audio (iOS): AAC, MP3, M4A, WAV
  - Archive files: 7z (view, extract)
- **View only (when shared with external app):**
  - Images: JPG, JPEG, PNG, GIF (not animated), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Documents: DOC, DOCX, PAGES
  - Spreadsheets: XLS, XLSX, CSV, NUMBERS
  - Presentations: PPT, PPTX, KEY

- Rich Text: RTF
- Video: MOV, MP4, M4V

Note that external apps are not be able to decrypt encrypted files.

If Sophos Secure Workspace is managed by Sophos Mobile, you can additionally view, edit and create files of the following types:

- **View (with the integrated Polaris Office library):**

  File formats written in italics are only supported by the Android version.

  - Microsoft Word 97-2013: DOC, DOCX, *DOT*, *DOTX*
  - Microsoft Excel 97-2013: XLS, XLSX, *XLTX*, *CSV*
  - Microsoft PowerPoint 97-2013: PPT, PPTX, *PPS*, *PPSX*, *POT*, *POTX*
- **Edit (with the integrated Polaris Office library):**
  - Microsoft Word 97-2013: DOC, DOCX
  - Microsoft Excel 97-2013: XLS, XLSX
  - Microsoft PowerPoint 97-2013: PPT, PPTX
- **Create (with the integrated Polaris Office library):**
  - Microsoft Word 2013: DOCX
  - Microsoft Excel 2013: XLSX
  - Microsoft PowerPoint 2013: PPTX

28 Related Sophos products

Find more information about related Sophos products on the internet:

- Sophos Mobile: https://www.sophos.com/en-us/products/mobile-control.aspx.
- Sophos SafeGuard Encryption: https://www.sophos.com/en-us/products/safeguard-encryption.aspx.
- Sophos Antivirus and Security for Android: https://play.google.com/store/apps/details?id=com.sophos.smsec.

29 Support

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

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

30 Legal notices