SOPHOS

Cybersecurity
made
simple.

Sophos Intercept X for Mobile

Help (Android)

product version: 9.6

Contents

1 Accessibility

Sophos Intercept X for Mobile is compliant with the Web Content Accessibility Guidelines (WCAG) 2.1 level AA. You can find more information on these guidelines in related information.

We recommend that you use Sophos Intercept X for Mobile with TalkBack, the Google screen reader included on Android devices. You can find a link for using TalkBack in related information. If you need further help with TalkBack, you can contact Google technical support.

If you want to use assistive technology products with our software we recommend that you are familiar with how your chosen product works and the available keyboard commands.

Known limitation

Due to a limitation of the Android OS, screen reader users can only use headings to navigate if they have Android 9 or later.

Related information

Web Content Accessibility Guidelines

Android accessibility help: Get started on Android with TalkBack

2 About Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protects your Android device and your privacy without impacting performance or battery life. With up-to-the-minute intelligence from SophosLabs, apps are automatically scanned for malware as you install them, to protect you from data loss and unexpected costs.

3 Dashboard

The Sophos Intercept X for Mobile dashboard gives you an overview of the device’s security status.

Features have different colors depending on their status:

- Green: No issues found
- Red: Issues found
- Blue: Feature is turned on
- Gray: Feature is turned off or not configured

4 Device security

Like all operating systems, Android lets you configure settings that make the device less secure. Sophos Intercept X for Mobile checks these security-related settings and gives recommendations for making your device more secure.

Note
When Sophos Intercept X for Mobile is managed by Sophos Mobile, security-related system settings are configured by your organization.

The settings listed under **Device security** have different colors depending on their status:

- Green (Secure): The setting ensures the maximum possible device security.
- Red (Insecure): The setting might lead to security issues. Follow the recommendations to change it.
- Yellow (Unknown): Android devices have different settings depending on the device model and the Android version. If Sophos Intercept X for Mobile can’t determine if the setting is insecure, it’s shown in yellow. Consider changing it.
- Gray (Turned off): Checking is turned off. The setting is not taken into account when determining the device security status.

Tap a setting to change it or to learn more about how it impacts device security.

4.1 Update Advisor

Update Advisor displays information about your Android version and checks if newer versions are available.

Update Advisor uses Sophos installation statistics to find out if a newer Android version is available for your device.

To open Update Advisor, select **Latest Android version** on the **Device security** page.

We recommend you install updates automatically. If your device has an optional setting to do this, tap **Check settings** and turn on automatic updates in the **Settings** app of the device.

5 Web Filtering

You use Web Filtering to specify types of websites you want to be warned about before opening them. This protects you from browsing sites with malicious, undesirable or illegal content.

Configure Web Filtering

On the dashboard, Web Filtering is available under **Network security**.

- On the **Web Filtering** page, turn on Web Filtering.
- To enable malicious website filtering, tap **Malicious content** and select **Warn** or **Block**.
- To enable filtering of websites that fall into a certain category, tap the category and select **Warn** or **Block**.
- **Allow list:** You can suppress the warning for certain malicious or categorized pages permanently. This is useful if one of the pages you visit frequently falls into a category that triggers a warning or is blocked. Select **Always allow access to this page** in the **Web Filtering** warning dialog. To filter such pages again, tap **Clear allowed pages list**.

Tip
To test website filtering, Sophos has created the site sophostest.com containing example pages for each category. Although some of these pages are classified as potentially offensive or dangerous, the page content itself is harmless in all cases.

Supported web browsers

Web filtering protects you when you use one of the apps listed under **Protected browsers**.

Supported browsers:

- Google Chrome
- Firefox
- Android web browser
- Microsoft Edge

Under **Protected browsers (not tested)** apps are listed which may work, but have not been tested.

Tip
If a supported web browser is installed on your device but is not listed under **Protected browsers**, check that Sophos Accessibility Service is turned on (in the system settings under **Accessibility**).

6 Link Checker

You use Link Checker to check links in an email or document for malicious or inappropriate content.

Link Checker processes all links you tap in non-browser apps. You use Web Filtering to check links on a web page. See Web Filtering (page 5).

On the dashboard, Link Checker is available under **Network security**.

To set up Link Checker:

1. On the **Link Checker** page, turn on Link Checker.
2. Select your regular browser app for opening web links.
3. The first time you tap a link after you've turned on Link Checker, Android asks you to select an app for opening the link. Select **Sophos Link Checker**.

When you tap a link, it's passed on to Link Checker and checked for malicious or inappropriate content based on the classification provided by SophosLabs. Afterward, the link is opened in your browser.

Note
Link Checker can't check links in apps that open them internally instead of passing them on to the browser app. If the app lets you choose how to open web links, use the browser so that Link Checker can process the link.

For example in Gmail, the setting is called **Open web links in Gmail**. Turn that setting off to let Link Checker check links in your email messages.

7 Wi-Fi Security

You use Wi-Fi Security to check your Wi-Fi connection for network-based threats.

Note
If Sophos Intercept X for Mobile is enrolled with Sophos Mobile, this feature is managed by your organization.

On the dashboard, Wi-Fi Security is available under **Network security**.

Issue types

Sophos Intercept X for Mobile detects the following issues:

ARP spoofing	ARP spoofing is where an attacker sends malicious Address Resolution Protocol (ARP) messages to your computer, making it believe the attacker’s MAC address is associated with the IP address of your network gateway. This allows them to access your private network, steal sensitive data, and launch additional attacks like denial-of-service or man-in-the-middle attacks.
Captive portal	A captive portal is a way for public Wi-Fi networks to ask for authentication before granting access to the network. Because all traffic is redirected to the captive portal, you might receive additional warnings.
Content manipulation	Content manipulation is where an attacker manipulates a website’s content to force you to do harmful actions. This allows them to do such things as bypass authentication or delete data.
SSL interception	SSL interception is where an attacker uses a false server certificate to intercept the secured connection between your computer and a website. The attacker can decrypt sensitive data while letting you believe your connection is still secure.
SSL stripping	SSL stripping is where an attacker downgrades the connection to a website from secure HTTPS to insecure HTTP. The attacker can redirect all traffic between your computer and the website via their own proxy server. This allows them to decrypt sensitive data while letting you believe you’re still connected via HTTPS.

Run checks

- To check the Wi-Fi network you are connected to, tap **Check Wi-Fi**.

- To automatically perform network checks in the background, turn on **Background check**. This runs a check every time the device connects to a Wi-Fi network.

8 App security

You can scan your device for malicious apps or files.

Sophos Intercept X for Mobile scans the device for malware and reports any malicious or potentially unwanted apps. The scanner uses an online lookup to check apps against the latest threat data in the SophosLabs cloud database as well as a built-in full-featured scan engine for improved detection whether the device is online or offline. The antivirus data is constantly updated by SophosLabs, who analyze Android threats 24 hours a day.

Perform scans

Sophos Intercept X for Mobile scans apps when they are installed. Additionally, you can configure scheduled scans and run manual scans.

To configure scheduled scans:

In the app settings, select **Scheduled scans** and then select a scan interval in **Scheduled scan interval**. You can also configure which parts of the device are scanned and which types of apps are reported.

To run a manual scan:

On the **App security** page, select **Show scan details** and then **Start**.

View scan results

On the **App security** page, an overview of the scan results is displayed under **App security issues**.

To view the individual issues, select **Show scan details**.

To view even more details about an issue, select an app listed under **Threats and PUAs** to open its **Object details** page. On that page, you can do the following:

- View how the app was installed and which permissions it requested.
- View a threat description.
- Open a web page with detailed threat information in your browser.
- Uninstall the app.
- Allow the app.

Related reference

Settings (page 22)

9 Authenticator

You use Authenticator to generate one-time passwords (also called verification codes) to sign in to your accounts that use multi-factor authentication.

Check with your account provider if multi-factor authentication is supported and how to enable it for your account.

Authenticator supports **time-based** and **counter-based** one-time passwords. See About one-time passwords (page 10).

To start Authenticator, touch and hold the Sophos icon and then tap **Authenticator**.

Features:

- For **time-based** passwords, Authenticator shows the currently valid one-time password together with an animated icon that depicts the remaining time until the code becomes invalid and the next code is calculated.
- For **counter-based** passwords, tap **Refresh** ↻ next to the account item to generate a new one-time password. To prevent you from accidentally generating multiple codes in a row, there is a latency of a few seconds after each generation before you can generate the next code.
- To copy the current one-time password for an account to the clipboard, tap and hold the account item and then tap **Copy** ⧉.
- To edit the account details, tap and hold the account item and then tap **Edit** ✎. For security reasons, you cannot display or edit the secret key.
- To delete an account, tap and hold the account item and then tap **Delete** 🗑.

Warning
When you delete an Authenticator entry, you will lose the ability to generate one-time passwords for that account. This doesn’t turn off multi-factor authentication. Deleting the Authenticator entry may prevent you from signing into your account.

Before you delete an entry, ensure that you either have an alternative mechanism for generating one-time passwords, or an alternative mechanism to sign in to your account without multi-factor authentication.

9.1 About one-time passwords

One-time passwords (also called verification codes) are composed of a number of digits. They are calculated from these parameters:

- A shared secret key that only your account provider and you know.
- Configuration values that are specific to your account provider.
- A consecutive counter.

When you use a one-time password to authenticate yourself, your account provider expects a password that is calculated from a certain counter value. Because Authenticator uses the same rules as your account provider to determine the current counter value, the provider will accept your one-time password.

Authenticator supports **time-based** and **counter-based** one-time passwords. These types differ in the way the current counter value is determined:

- **Time-based one-time passwords** (TOTP, according to RFC 6238): The counter value is incremented continuously based on the current time. The next value in the series of verification codes is generated when a defined time period has elapsed.
- **Counter-based one-time passwords** (HOTP, according to RFC 4226): The counter value is incremented on demand. The next value in the series of verification codes is generated when you request it.

9.2 Add account from QR code

Use this procedure if you have enabled multi-factor authentication for an account and your account provider has given you a QR code with the configuration details.

1. Tap **+** and then **Scan QR code**.
2. Scan the QR code with your device.

After the app has read the configuration details from the QR code, it sets up a new Authenticator account.

9.3 Add account manually

Use this procedure if you have enabled multi-factor authentication for an account and your account provider has given you a list of configuration details.

1. Tap **+** and then **Add manually**.
2. In the **Name** field, type a name for the new Authenticator account.
3. In the **Key** field, type the secret key that your account provider has specified. The key is specific to your account and constitutes the calculation basis for the one-time passwords.
4. In the **Type** field, select the calculation type that your account provider has specified.
5. If your account provider has specified additional settings, tap **Advanced** to display additional input fields.

   CAUTION
   Only fill in information that your account provider has specified.

   - In the **Issuer** field, enter a string that indicates the provider the account is associated with.
   - In the **Time period** field, enter the validity period in seconds. Only available for time-based one-time passwords.
   - In the **Counter** field, enter the initial counter value. Only available for counter-based one-time passwords.
   - In the **Code length** field, select the number of digits of the one-time passwords.
   - In the **Hash algorithm** field, select the hash algorithm for the calculation of the one-time passwords.
6. Optional: In the **Background color** field, select a color for the account entry, to easily identify it in the account list.
7. When you are ready, tap **OK** ✓.

This sets up a new Authenticator account.

10 Password Safe

You use Password Safe to store all your account data in a single place that is secured by a master password.

To start Password Safe, touch and hold the Sophos icon and then tap **Password Safe**.

You have the following options:

- Create a new Password Safe file.
- Import an existing KeePass KDBX file. When you edit password entries, only the local copy is changed.

Turn on AutoFill Passwords

In iOS 12 and later, you can use Password Safe to autofill passwords.

To turn **AutoFill Passwords** on for Password Safe:

1. Go to the **Settings** app and scroll down to **Passwords & Accounts**.
2. Tap **AutoFill Passwords** and turn on **AutoFill Passwords**.
3. Select **Intercept X** under **Allow filling from:**.

You can now access Password Safe by just tapping **Passwords** on the QuickType bar above the keyboard when you are prompted to enter credentials.

10.1 Create Password Safe entry

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

1. In Password Safe, tap **+**.
2. Select the type of entry you want to create:
    - **Add account entry** creates an entry with predefined fields suitable for web accounts and similar items.
    - **Add credit card entry** creates an entry with predefined fields suitable for credit cards and similar items.
    - **Add group** creates a folder within Password Safe to organize your entries.
3. Enter your data into the fields of the entry.
4. Optional: Tap **Add field** to add a custom field to the entry.

    If you turn on **Protected** for a custom field, you must tap the eye button next to the field to view the value. Also, protected fields are excluded from search results.
5. Tap the **Disk** icon to save the entry.

You can easily use the password data to sign in to a web page or app. See Use password data to sign in (page 13).

10.2 Generate passwords

1. Open the Password Safe entry for which you want to generate a password.
2. Tap **Edit** ✎ to switch to edit mode.
3. Tap **+** next to the password field to open the password generator.
4. Define the password length and the types of characters that must be included in the password.
5. Tap **Generate password** to generate a password based on your specification.
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.

10.3 Use password data to sign 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, tap it. To copy the URL to the clipboard instead, tap and hold it.

Tip
Every time you open a Password Safe entry, a notification is added to the Android notification area. From that notification, you can copy the user name and password values to the clipboard.

10.4 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** 📋.

10.5 Search Password Safe entries

In Password Safe, you can search for entry and group names, and for values of entry fields.

Note

You can’t search for password fields or fields you’ve configured as **Protected**.

1. In Password Safe, tap **Search** 🔍 to switch to search mode.
2. Enter a search string. The list of results is updated as you type.

10.6 Back up Password Safe

It’s important that you regularly back up your Password Safe file. If you lose the Password Safe file, for example because you’ve accidentally deleted it or lost your device, you can’t access your password data unless you have a recent backup copy.

1. In Password Safe, tap **More** ⋮ and then tap **Export**.
2. Select the app to which you want to export the Password Safe file.

   A copy of the Password Safe file is shared with the app you selected.

Note

We recommend you write down the location of the backup copy and store that note in a secure location.

11 QR Code Scanner

You use QR Code Scanner to scan QR codes and then process the embedded information.

To start QR Code Scanner, touch and hold the Sophos icon and then tap **QR Code Scanner**.

Web addresses

When you scan the QR code, the embedded URL is checked for malicious or inappropriate content based on the classification provided by SophosLabs.

- When the URL is reported as safe, tap **Open** to open it in your web browser.

Contacts

Scan the QR code and then:

- Tap **Add contact** to create an entry in your contacts using the embedded business card information.
- Tap **Show in map** to show the embedded location in your map app (Google Map by default).
- Tap **Dial number** to make a phone call to the embedded number. If the QR code contains more than one phone number, they are used in this order:
  1. Mobile phone number
  2. Work phone number
  3. Home phone number
- Tap **Send email** to create a new email to the embedded email address. If the QR code contains more than one email address, all of them are added to the **To** field.

Additional information
Sophos Intercept X for Mobile can read business card information in vCard 2.1 and 3.0 formats.

Wi-Fi configurations

Scan the QR code and then tap **Connect to network** to connect to the Wi-Fi network that is configured in the QR code.

Note
You are warned if you try to connect to an insecure network, i.e. a network that is not secured by WPA or WPA2.

12 App Protection

You use App Protection to configure a list of apps that can only be opened after you have authorized yourself. This is useful, for example, if you want to hand over your device to somebody else, to prevent them from using certain apps.

> **Note**
> When Sophos Intercept X for Mobile is managed by Sophos Mobile, App Protection is not available. App access is managed by your organization.

1. In the app menu, select **App Protection**.
2. In **Base configuration**, turn on App Protection.
3. The Intercept X app must be an Android device administrator. If you have not activated this yet, you are forwarded to the relevant Android **Settings** page. Tap **Activate**.
4. Select an authentication type for **App Protection**.

   You can choose from **Pattern**, **PIN**, **Password** and **Fingerprint** (if your device has a fingerprint sensor).

   > **Note**
   > When Sophos Intercept X for Mobile is managed by Sophos Mobile, the administrator can turn off fingerprint authentication.

5. Some task managers can disable **App Protection** by terminating its process. For task manager protection you need to install the Sophos Security & Antivirus Guard app. A message in **Base configuration** points this out. Tap the message to open the app in Google Play and then install it.
6. Tap **Grace period** and select the length of time for which your password is remembered when you exit an app and enter it again.
7. **Protect configuration** lists apps that can be used to uninstall or otherwise disable app protection. You can also protect Google Play and other installers to prevent the uncontrolled installation of apps on the device.
8. Swipe left. The **App selection** view is displayed. You can:
   - Select apps in the **Unprotected** list to protect them. The apps are displayed in the **Protected** list.
   - Deselect apps in the **Protected** list to remove protection. The apps are displayed in the **Unprotected** list.

Sophos Security & Antivirus Guard monitors the **App Protection** processes and restarts them if necessary.

> **Note**
> If you did not install Sophos Security & Antivirus Guard and leave the **App Protection** settings, you are prompted again to install it. It is highly recommended to do so.

13 Privacy Advisor

Privacy Advisor displays information about the permissions the apps installed on your device have.

Note
This section describes Privacy Advisor for Android 6 and later. For Privacy Advisor for Android 5, see Privacy Advisor (Android 5) (page 19).

Android permission handling

Permissions are a central security mechanism of Android that grant an app certain rights. With version 6, Android has changed the way apps ask for permissions:

- Apps that are created for Android 6 or later ask you to grant a permission **at run time**, that is when you access a feature of the app that needs a permission you have not granted yet.
- Apps that are created for Android 5 or earlier (referred to as legacy apps) ask for all required permissions **at install time**. When a legacy app is installed on Android 6 and later, you can deny individual permissions. But because the app is not designed to handle this, it may stop working.

What you can see in Privacy Advisor

Privacy Advisor shows you the status of permissions that are classified by Google as dangerous because they affect your privacy or the operation of other apps:

- **Calendar permission** 📅 **Calendar**
- **Camera permission** 📷 **Camera**
- **Contacts permission** 📇 **Contacts**
- **Location permission** 📍 **Location**
- **Microphone permission** 🎤 **Microphone**
- **Phone permission** 📞 **Phone**
- **Body sensors permission** 🏃 **Body sensors**
- **SMS permission** 💬 **SMS**
- **Storage permission** 📁 **Storage**

A permission can have one of the following states:

- **Granted** 📷 Requested and granted
- **Denied** 🚫 Requested and denied

Note
For legacy apps, permissions are always shown as “Requested and granted”, even if you have turned off the permission in the app settings.

What you can do in Privacy Advisor

- To view details of all permissions an app requested (including non-dangerous permissions): Tap the app icon.
- To grant or deny a permission: Tap the app icon and then tap **Change permissions** to open the app's **App info** page. From there, tap **Permissions**.
- To display the history of changes you made to permissions: Tap **Permission change history** in the title bar.
- To configure what you see in Privacy Advisor: Tap **Filter**. You can exclude certain permissions or apps of a certain type, like system apps or legacy apps.
- To change the app order: Tap **Sort** and then select how the apps are sorted.

14 Privacy Advisor (Android 5)

Privacy Advisor displays information about the permissions the apps installed on your device have.

Note

This section describes Privacy Advisor for Android 5. For Privacy Advisor for Android 6 and later, see Privacy Advisor (page 17).

There are three permissions filters:

- **Apps that may cause costs**

  Some apps can cause additional costs. Depending on the permissions an app requests, the app may be able to call premium-rate telephone numbers, change the network state of your phone (which may cause costs when your phone is in roaming mode) or send text messages without your confirmation.

- **Apps that may harm your privacy**

  Your smartphone or tablet contains private information. Apps with certain permissions can read your contact list. You cannot control what the app is actually doing with this information as you have granted the app the permission to do so. Combined with certain connectivity permissions, an app could easily send all your contact information to a third party without you having to confirm this action. Such apps can harm your privacy.

- **Apps that may access the internet**

  Currently, most of the apps available need permission to connect to the internet. In combination with other permissions, this can be a huge security issue for you. Information that is sent to and received from the internet cannot be monitored. Check if internet access is needed for an app and if the app is trustworthy.

Privacy Advisor lists all apps installed on the device. At the bottom of the screen, icons for the three Privacy Advisor filters are displayed. Tap an icon to enable or disable the respective filter.

Filters can be combined so that all apps having permissions related to the filters currently selected are highlighted.

The listed apps are ranked based on how the app's permissions are related to the selected filters:

- Apps shown in red: The permissions the app requests indicate a high risk for the selected filter.
- Apps shown in yellow: The permissions the app requests indicate a normal risk for the selected filter.
- Apps shown in white: The permissions the app requests indicate a low risk for the selected filter.

Tap a list entry to display detailed information about the app. The display shows which permissions the app has and what the permissions may be used for.

If you want to uninstall the app from your device, tap **Uninstall**.

15 Corporate management

In a corporate environment, Sophos Intercept X for Mobile can be managed by Sophos Mobile. This allows your organization to monitor your device’s compliance status.

To enroll Sophos Intercept X for Mobile with Sophos Mobile, follow the instruction you received from your organization.

When Sophos Intercept X for Mobile is managed by Sophos Mobile, the following differences apply:

- App settings are defined centrally by your organization.
- Your organization can trigger scans to determine the security status of your device.
- If your device becomes non-compliant with your organization’s policy, network access or other features might be restricted. You can view the compliance status on the app’s dashboard. See Resolve compliance violations (page 20).

Note
Alternatively, your organization can manage your device, or a work area on your device, with the Sophos Mobile Control app. This gives your organization even more control, such as installing or uninstalling apps, or turning off device features. In this case, you can view the compliance status of your device and contact IT through the Sophos Mobile Control app. For details, see the Sophos Mobile user help.

15.1 Resolve compliance violations

When Sophos Intercept X for Mobile is managed by Sophos Mobile, the dashboard shows the compliance status based on your organization’s policy.

To view and resolve compliance violations:

1. On the dashboard, tap **Corporate management**.

   When there are compliance violations, the tile has a red icon.
2. Tap the compliance violation and follow the instructions to resolve it.

Note
When your device is non-compliant, network access or other features might be restricted.

15.2 Get support

When Sophos Intercept X for Mobile is managed by Sophos Mobile, you can display details about how to contact IT and any further information provided.

On the dashboard, tap **Corporate management**.

Contact details are displayed under **IT contact** and **Additional info**.

Tip
You can tap the **Email**, **Phone** or **Mobile** fields to write an email or make a phone call to IT.

16 Settings

Setting	Description
Scheduled scans	Perform automatic periodic scans.
Scheduled scan interval	The frequency of scheduled scans. If you select **Daily while charging**, a scan is performed when the device is connected to a power supply for more than 30 minutes.
Manage allowed apps	Tap to show the list of allowed apps. These apps are not shown in the scan results. You can remove apps from this list. Any apps you remove are shown in the **Threats and PUAs** list again.
Clear defaults	Tap to stop using Intercept X as default app to open supported links.
Scan system apps	Select this to include Android system apps in scanning. System apps are not scanned, by default, as they are protected by Android and can’t be removed by the user.
Scan storage	Select this to include the SD card and USB storage devices in scanning.
Detect PUAs	Select this to turn on the detection of potentially unwanted apps (PUAs). PUAs are apps that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are adware, dialer, system monitor, remote administration tools and hacking tools. However, certain apps that fall into the PUA category might be considered useful by some users.
App reputation	Select this to turn on the detection of low reputation apps. Low reputation apps are apps that have a low reputation based on Sophos Live Protection data.
Scan notification	Select this to turn on scan notifications for clean apps. If this is deselected, you only get notifications for malware, PUAs, and low reputation apps. Sophos Intercept X for Mobile scans apps during installation on the Android device or when apps are launched from the SD card or USB storage devices. You find the notifications in the Notification Panel.
Monitor storage	Select this to scan all new apps and files that are downloaded or copied to the SD card or USB storage devices. For all newly attached storage devices a scan is initiated automatically.

Setting	Description
Version	The version of the antivirus engine and antivirus data.
Last update	The date when antivirus data was retrieved from Sophos. Tap to check for updates.
Update mode	This setting defines the data connection Sophos Intercept X for Mobile uses to download updates of the virus detection data.
Send log by email	Tap to send an email with the app’s log file attached. The email address of Sophos Support is inserted by default.
Track data to help improve usability	Allow Sophos to collect anonymous usage data to improve the app.
Uninstall Sophos Intercept X for Mobile	Tap to uninstall the Intercept X app and the associated Security & Antivirus Guard app, if installed.

17 Back up and restore

You can back up the app settings, for example to use them on another device.

You can back up the following items:

- Settings
- Scanner
- Web Filtering
- App Protection
- Authenticator

When Sophos Intercept X for Mobile is managed by Sophos Mobile, you can only back up Authenticator accounts.

Back up settings

1. In the app menu, select **Back up & Restore**.
2. Tap **Back up**.
3. Select the settings you want to export.
4. Tap **Back up**.
5. Enter your device credentials and tap **Next**.
6. Select the location to create the backup copy.

   Tip
   Save the backup to your cloud storage so you can use it on other devices.

7. Enter a name for the file and tap **Save**.
8. Enter a password for the backup copy, confirm it, and tap **OK**.

Restore settings

1. On the **Back up & Restore** page, tap **Restore**.
2. Go to the location where you saved the file and tap the backup copy.
3. Enter the password for the backup copy and tap **OK**.
4. Select the settings you want to restore.
5. Tap **Restore**.

18 Logging

Sophos Intercept X for Mobile records important operations in its own log. This is in addition to the Android log. You do not get direct feedback about the results of the background operations the app performs, such as malware scans when you install other apps. The log provides a detailed report about these actions. It details when these actions were performed and the relevant results.

- To display the log, tap **Menu** ≡ and then tap **Log**.
- To clear the log, tap **Delete** 🗑 in the title bar.

19 Legal notices