SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile Help (iOS)

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 the VoiceOver screen reader and the Zoom magnifying software included on iOS devices. You can find links for using VoiceOver and Zoom in related information. If you need further help with VoiceOver or Zoom, you can contact Apple 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.

Related information

Web Content Accessibility Guidelines

iPhone user guide: Turn on and practice VoiceOver on iPhone

iPhone user guide: Zoom in on the iPhone screen

2 About Sophos Intercept X for Mobile

Sophos Intercept X for Mobile helps you to work safely on your iPhone or iPad.

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.

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

Under **Device security** you can see the device's health status.

Sophos Intercept X for Mobile shows the following information:

- General device information like the model name and the iOS version.
- Update recommendations if you don't have the latest available iOS version installed.
- Jailbreak information if Sophos Intercept X for Mobile has detected a jailbreak on the device.

5 Web Filtering

Your organization can use Web Filtering to protect you from browsing sites with malicious, undesirable or illegal content.

If your organization manages your device, it can specify types of websites you should be warned about before opening them or block websites. This protects you from browsing sites with malicious, undesirable or illegal content.

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

Note

- Your organization must turn this feature on.

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. Swipe down the **Web request blocked** notification and tap **Add to allow list**.

Under **Allow list** the number of allowed pages is displayed. Tap the counter to display all pages.

Entries you have added and those predefined by your organization are displayed in separate sections.

To filter a page again, swipe left the entry to delete it. You can only do this for entries that you have added yourself.

Block list

You can add web pages for which a warning is raised to a block list so that they are always blocked. Swipe down the **Web request blocked** notification and tap **Add to block list**.

Under **Block list** the number of blocked pages is displayed. Tap the counter to display the entries for all pages.

Entries you have added and those predefined by your organization are displayed in separate sections.

To raise a warning again, swipe left the entry to delete it. You can only do this for entries that you have added yourself.

6 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. ARP spoofing can't be detected on devices with iOS 10.3 or later.
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.

Hide issues

You can hide Wi-Fi issues for specific networks. Hidden issues don’t contribute to the device’s health status.

To show all issues again, select **Show all Wi-Fi issues** in the app settings.

7 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 8).

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 **Tap for code** to create the first code, or **Next** to create the next code. 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 it.
- To edit the account details, tap **Edit**, select the account item and then tap **Modify**. For security reasons, you cannot display or edit the secret key.
- To delete an account, tap **Edit**, select the account item and then tap the **Delete** icon.

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.

7.1 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.

7.2 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. Select **Create > 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.

7.3 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. Select **Create > 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, enter these in the following fields.

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

   - In the **Time period** field, enter the validity period in seconds. Only available for time-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 **Save**.

This sets up a new Authenticator account.

8 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.
- Open an existing KeePass KDBX file. When you edit password entries, the original file 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.

8.1 Create Password Safe entry

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

1. In Password Safe, tap **Plus** ⊕.
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.
   - **Notes** creates an entry for taking a secure note.
   - **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 **Plus** ⊕ and then 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.

   With **Plus** ⊕ you can also add a file or a picture to the entry.
5. Tap **Done** 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 11).

Note
You might experience performance issues when you attach large files or a large number of files to an entry. We recommend you encrypt such files with the Sophos Secure Workspace app to store them securely.

8.2 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 the **Cogwheel** icon to open the password generator.
4. Define the password length and the types of characters that must be included in the password.
5. Tap **Refresh** 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.

8.3 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 Safari, tap the **Globe** icon next to the **URL** field.

8.4 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**.

8.5 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**.

Tip
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.

1. In Password Safe, swipe down to switch to search mode.
2. Enter a search string. The list of results is updated as you type.

8.6 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 the Password Safe tile of the app's dashboard, tap **Info** ⓘ.
2. Tap **Back Up Password Safe File**.
3. Select the location to create the backup copy.

Note
We recommend you also print a recovery sheet that helps you access your password data, for example if you've forgotten your master password or lost your key file. See Print Password Safe recovery details sheet (page 12).

8.7 Print Password Safe recovery details sheet

If you forget the Password Safe master password or lose the key file, you can't access the data stored in the Password Safe. To prevent this, print a recovery details sheet that contains the required information.

Warning
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, the recovery details sheet alone is not sufficient to retrieve your password data. See Back up Password Safe (page 12).

1. In the Password Safe tile of the app's dashboard, tap **Info** ⓘ.
2. Tap **Print recovery details sheet**.
3. Select the printer and the number of copies, and then tap **Print**.

4. In the printout, fill in the following information:
   - Your master password
   - The location of your Password Safe file
   - The location of your backup copy
5. Store the recovery details sheet in a secure location.

   Everyone with access to the recovery details sheet and to your Password Safe file can read your password data.

If you've secured the Password Safe file with a key file, a fingerprint of that file is included in the recovery details sheet, in the form of a QR code. You can use that QR code as an alternative to the actual key file to open your Password Safe file.

9 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 **Continue** to open it in Safari.

Contacts

Scan the QR code and then tap **Add** to create an entry in your contacts using the embedded business card information.

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 **Copy** to copy the password to the clipboard. In the **Settings** app, go to **Wi-Fi**, select the network and paste the password when prompted.

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.

10 Message Filtering

Your organization can use Message Filtering to check your incoming SMS/MMS messages for phishing URLs.

Suspicious messages are filtered into a separate **SMS Junk** tab.

If you see **Turn on Message Filtering** in the app settings, you need to turn on message filtering in the **Settings** app as required by your organization.

Turn on message filtering

Go to your iOS **Settings** app, go to **Messages**, tap **Unknown & Spam** and turn on **Intercept X** under **SMS Filtering**.

SMS Junk tab in Messages app

If a message from an unknown sender is classified as spam, the message is moved to the **SMS Junk** tab in the Messages app. Existing and further messages from the same sender are moved to **SMS Junk** as well.

Note

- Messages from a known contact are never classified as spam.
- Message Filtering does not work for iMessages.

11 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.
- 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 16).

11.1 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.

11.2 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**.

12 Settings

Setting	Description
Turn on Message Filtering	Check incoming SMS/MMS messages for phishing URLs. Your organization must turn this feature on. See Message Filtering (page 15).
Turn on Web Filtering	Block connections to malicious or categorized web pages. Your organization must turn this feature on. See Web Filtering (page 5).
Show all Wi-Fi issues	Show all Wi-Fi issues, including the issues you've previously 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.

13 Back up and restore

You can back up your Authenticator accounts, to move them to a new iOS or Android device.

Back up accounts

1. In the app menu, select **Back up & Restore**.
2. Tap **Back up**.
3. Enter a name for the backup copy.
4. Enter a password, confirm it, and tap **OK**.
5. Select the location to create the backup copy.

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

6. Tap **Add**.

Restore accounts

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**.

14 Legal notices