WEBROOT
SecureAnywhere®

Mobile Security for Android User Guide

Copyright

WSA Mobile Security for Android User Guide

Table of Contents

Chapter 1: WSA Mobile Security for Android User Guide

To get started using the Mobile Security for Android User Guide, see the following topic:

WSA Mobile Security for Android User Guide Overview

After you install the product and create an account, SecureAnywhere Mobile immediately begins protecting your Android device.

Note: WSA Internet Security Plus includes all features except Backup &Sync. For a comparison of products, see our product comparison for consumer products.

- Scans your device after account creation, then scans again on a weekly basis; cloud definitions are always up to date. A threat definition is a set of fingerprints that characterizes viruses, spyware, and other types of unwanted items. To change the scan schedule, see *Changing Scan Schedules on page 19*.
- Alerts you immediately if it encounters potential security issues. To learn more, see *Responding to Alerts on page 30* and *Checking the Status and History of Mobile Devices on page 9*.
- Monitors all newly installed memory cards and applications for threats. To learn more, see *About Shields on page 15*.
- Monitor all visited websites for malware and phishing attempts, and blocking potentially malicious sites. To learn more, see *Using SecureWeb Browsing on page 10*.
- Blocks unwanted calls and texts. To create a blocked list, see *Enabling or Disabling Call & SMS Blocking Features on page 31*.
- Protects your device if it's lost or stolen. To learn more, see *Using Lost Device Protection on page 24*.

Chapter 2: Managing Your Account

To manage your account, see the following topics:

Registering Mobile Security for Android

If you have the Premier or Complete versions of SecureAnywhere Mobile, you must register the product to activate all the features.

Note: WSA Internet Security Plus includes all features except Backup &Sync. For a comparison of products, see our product comparison for consumer products.

To register your product:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. In the Settings panel, tap **Register**.
3. Tap **Activate**.
4. Enter your product key, then tap **Activate**.

System Requirements for Android

The following describes the system requirements for using Mobile Security functionality on an Android device.

Operating Systems

- Android operating system version 4.4 (Kit Kat) or higher.

Devices

- Android-compatible phones and tablets, including Kindle and Nook.
- Requires an active internet connection for some features. For a list of these features, click here.

Changing Account Settings

SecureAnywhere Mobile has several settings that you can change:

- The password for your account.
- The persistent status of the Webroot icon in the notification bar.
- The phone number stored in SecureAnywhere Mobile.
- The settings for Webroot Automated Research Network (WARN). WARN is a global community that provides Webroot with sample items detected during scans and shielding, which helps us identify and fight emerging threats.

Note: WSA Internet Security Plus includes all features except Backup &Sync. For a comparison of products, see our product comparison for consumer products.

To change your account password:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. Tap **Change Password**.
3. Enter your current password and then a new password.
4. Tap **OK**.

To change the persistent status of the Webroot icon:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. Tap **General Settings**.
3. Tap the **Persistent Status** checkbox.
   - A green checkmark indicates that the Webroot icon will display in your device's top bar.
   - A grayed-out checkmark removes the icon from the top bar.

To change the phone number stored in Webroot Mobile Security:

1. Go to https://my.webrootanywhere.com and log in using your email address and Webroot password.
2. Click on the name of the device.
3. In the About tab, click on **Edit** next to the phone number.
4. Enter the new number and click **Save**.

To disable WARN:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. In the Settings panel, tap **General Settings**.
3. Tap the **WARN Enabled** checkbox, so that the checkmark is grayed out.

Checking Statuses

You can check the device's status from the app or from the SecureAnywhere website.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

From the Device App

The Webroot icon displays on the Home panel of your device. either the top or bottom. The indicator on the Webroot icon turns yellow or red when SecureAnywhere Mobile needs to alert you about a system status. You can see more details about the issue by tapping the icon or dragging the Android bar.

From the SecureAnywhere Website

In a web browser, go to https://my.webrootanywhere.com and log in using your email address and Webroot password. A panel opens that displays all the devices in your Webroot account. For each device, you can see the status and a history of activity.

Checking the Status and History of Mobile Devices

The SecureAnywhere website shows the status and history of each mobile device in your Webroot account.

Note: WSA Internet Security Plus includes all features except Backup &Sync. For a comparison of products, see our product comparison for consumer products.

To check status and history:

1. Go to https://my.webrootanywhere.com.
2. Log in using your email address and Webroot password. This must be the same email address and password that you used to create a Webroot account on your device.

   Note: If you don't remember your email address or password, click the **Can't log in?** link.

   At a glance, you can quickly see the status of all your devices.

3. To view more information about a device, click on the device name in the web page. A panel displays that displays additional more details.
4. At the top of the panel, you can click on the tabs for any of the following:
   - Security status
   - History of activity
   - Lost Device Protection commands

   For more information on using these commands, see *Using Lost Device Protection on page 24*.

Using SecureWeb Browsing

Secure Web Browsing allows you to safely surf the Internet by blocking malicious websites from loading before you access them. When you attempt to visit a website that is known for spreading malware, an alert opens and gives you the following options:

- Continue blocking the site
- Ignore the alert and proceed to the site
- Permanently ignore the warning and always proceed to the site

We recommend that you keep Secure Web Browsing enabled and continue blocking any sites that it categorized as potentially malicious.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To enable or disable Secure Web Browsing:

1. From the main SecureAnywhere Mobile panel, tap **Security** at the bottom.
2. Tap **Secure Web Browsing**. The Block known threats panel displays an ON button if the feature is turned on.
3. Tap the button to turn the feature on or off. Be aware that if you turn off Secure Web Browsing, SecureAnywhere Mobile warns you that your device is at risk by displaying a yellow exclamation mark.

   Note: Currently, SecureWeb Browsing is only supported on the default-packaged Android browser.

To review or edit the list of threatening sites you chose to ignore:

1. Tap **Ignored Websites** from the bottom of the Secure Web Browsing panel.
2. To remove a site from the Ignored Websites list, do one of the following:
   - Press and hold the site name until the Selected Ignore Item panel opens, then tap Stop Ignoring.
   - Tap the **Menu** button from the panel and tap Clear Ignore **List.**

   When a site is removed from the list, the Secure Web Browser will detect it again if you try to access it.

Using the App Inspector

You can use the App Inspector to identify any applications that may be compromising your privacy, costing you money, or draining your battery.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To use the App Inspector:

1. From the main SecureAnywhere Mobile panel, tap **Identity & Privacy** from the bottom.
2. Tap **App Inspector**.
3. Select from the following:
   - **Review Apps** — This option identifies any applications that may be a security concern. When the next panel opens, tap the **Forward arrow** to see the identified list of apps, which exhibit the following behavior:
     - Accessing messages from Short Message Service (SMS) and Multimedia Messaging Service (MMS). SMS is the text communication service used for your mobile device. MMS is an extension of SMS that allows for multimedia content, such as pictures and videos.
     - Making phone calls for additional costs, without prompting you.
     - Accessing information about your account, which could lead to identity theft.
     - Tracking your location through a network or Global Positioning System (GPS), a satellite-based navigation system.
     - When the scan completes, Webroot SecureAnywhere lists applications based on their security vulnerability. Some applications listed in the Costs category are legitimate and need access to the phone capabilities, while others do not and may be costing you extra money, for example, if you have a card game that is requesting permission to SMS functionality.
   - **Battery Monitor** — This option displays the following information:
     - **Battery Information** — The real-time statistics for your battery, such as its percentage of charge remaining, temperature, etc.
     - **Power Usage by App** — The percentage of battery power that each app uses, enabling you to determine which apps may be draining your battery. The Power Usage by App displays statistics over time.
     - **Current Usage** — Real-time usage statistics, available when you tap the Current Usage button at

the bottom of the panel. If the device is currently plugged into a USB or AC outlet, the stats are reported for the previous period of time when the device was running on a battery.

> **Note:** On the Battery Monitor, both the Power Usage by App and Current Usage functionality is only available on version 4.1, also known as Jellybean, and below.

- **Network Monitor** — This option displays which apps are currently accessing the network. It provides statistics for the network protocol used, the Local IP and Remote IP addresses, and port connection status. This information can help you discover rogue applications connected to remote hosts outside your country.

4. Click on a list item to query the Internet WhoIs database. This query provides the following information:
   - **Remote IP address**
   - **DNS name corresponding to this IP address**
   - **Country and region of the connection origin**
   - **IPS and organization for the remote hosts**
   - **Latitude and longitude of the remote hosts.**
5. Tap the **Pinpoint** button to view the host location via Google maps.

Uninstalling Mobile Security for Android

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To uninstall the Mobile Security for Android app:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. In the Settings panel, tap **Uninstall**.
3. If prompted, enter your Webroot password and tap **OK** to continue.
4. In the confirmation panel, tap **OK** to remove SecureAnywhere from your device.

Chapter 3: Working With Shields

To work with shields, see the following topics:

About Shields

SecureAnywhere Mobile contains active protection features called shields, which immediately alert you if they detect a potential threat or vulnerability. The following list describes each shield type.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

Install Shield

- Alerts you if a new or updated application contains a potential threat, and blocks it from installing.
- SecureAnywhere Mobile provides options for either removing it, that is, sending it to quarantine, or ignoring it and continuing with the download.

File System Shield

- Alerts you if the memory card in your device contains a potential threat, including threats that may launch when you restart or power on your device.
- If it detects a threat, it provides options for removing it, that is, sending it to quarantine, or ignoring it.

Execution Shield

- Alerts you if a suspicious application or file tries to install or start on your device.
- If it detects a threat, it provides options for preventing the item from running, that is, sending it to quarantine, or ignoring the warning and allowing the item to run.

Dialer Shield

- Blocks websites from dialing phone numbers that can cause suspicious or damaging activity, such as exposing your device's International Mobile Equipment Identity (IMEI) number, wiping your device, and so on.

Unknown Sources Shield

- Alerts you if the Unknown Sources setting is enabled.
- The Unknown Sources setting is a feature of your mobile device, available from Settings.
- If enabled, it allows you to download applications that are not part of the Android Market.

- On AT&T devices, the Unknown Sources setting is always secure, which means the setting is disabled.
- Premier/Complete versions only.

USB Debugging Shield

- Alerts you if the USB Debugging setting is enabled.
- The USB Debugging setting is a feature of your mobile device, available from Settings, which allows you to communicate with a computer over a USB port.
- Connecting via USB can make the mobile device vulnerable to malware that could be downloaded over this port.
- Premier/Complete versions only.

Changing Shield Settings

SecureAnywhere Mobile contains active protection features called shields, which immediately alert you if they detect a potential threat or vulnerability.

Use the following procedure to change shield settings.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To change shield settings:

1. From the main SecureAnywhere Mobile panel, tap **Security** from the bottom.
2. Tap **Antivirus**.
3. Tap **Shields** at the bottom.
4. To turn a shield on or off, tap the checkbox for the shield option.
   - A green checkmark indicates the setting is on.
   - A greyed-out checkmark indicates the setting is off.

   When you disable shield settings, SecureAnywhere Mobile displays a yellow warning. For a description of shield settings, see *About Shields on page 15*.

Chapter 4: Working With Scans

To work with scans, see the following topics:

Changing Scan Schedules

SecureAnywhere Mobile scans your device weekly; cloud definitions are always up to date. If needed, you can change the frequency of the scan schedule.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To change a scan schedule:

1. From the main SecureAnywhere Mobile panel, tap **Security** at the bottom.
2. Tap **Antivirus**.
3. Tap **Schedule** at the bottom.
4. Tap **Scan Frequency**.
5. In the next panel, tap one of the following:
   - **Never**
   - **Hourly**
   - **Daily**
   - **Weekly**

Running Scans

SecureAnywhere Mobile automatically scans your device on a weekly basis. Use the following procedure to scan your device immediately.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To run a scan:

1. In the main panel, tap **Scan for Threats Now**. SecureAnywhere runs a scan.
2. When the scan completes, tap **Finish** to view the following system statuses:
   - **Last scan** — Displays the date and time of the last scan. If a scan hasn't run in more than seven days, the status icon is yellow.
   - **Shields** — If all shields are enabled, displays ON. If one or more shields are disabled, a yellow icon displays along with a Fix button. To turn on all shields, tap **Fix**.
   - **Scheduled scans** — If scans are scheduled, it displays a green icon. If scans are not scheduled, a yellow icon displays along with a Fix button. To return the schedules to their default values, tap **Fix**. SecureAnywhere Mobile automatically scans your device on a weekly basis; cloud definitions are always up to date.
   - **USB Debugging setting** — Displays SAFE to indicate that the Android device's USB Debugging setting is in a safe mode, which means it will prevent the USB port from communicating with a computer. Premium/Complete versions only.
   - **Unknown sources setting** — Displays SAFE to indicate that the Android device's Unknown Sources setting is in a safe mode, which means it will not allow application installations from outside the Android Market. Premium/Complete versions only.

Chapter 5: Working With Lost Device Protection

To work with Lost Device Protection, see the following topics:

About Lost Device Protection

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

Lost device protection helps you locate a missing phone or tablet, and lock it down, if necessary. You can use another mobile device or the SecureAnywhere website to send the missing device one of these commands:

Lock

- Remotely locks the device and prevents its unauthorized use.
- Once the device is locked, you must use your account password to unlock it.

Wipe

- Immediately locks the device, then performs a factory reset to remove everything on your phone, including your personal data, your apps, and your account.
- Do not use this command unless you are absolutely sure that your device is permanently lost and you want to completely wipe it.
- Before wiping data, SecureAnywhere Mobile turns off the Auto-sync function so it won't delete anything you've previously uploaded to the Gmail servers, such as contacts or calendar entries.
- Available for the Premier/Complete version only.

Locate

- Locks your phone, the same as the Lock command, described above, then responds with a link to a Google Maps page displaying your phone's current location.
- For the Locate command to work, the device must have either a GPS, Wi-Fi, or a telephony connection.
- If your device does not support SMS or if Webroot does not support your carrier, then you must have logged into the Android Marketplace.

Scream

- Locks your phone, the same as the Lock command, described above, and then blasts a loud screaming noise from your phone to help you locate the device or scare a thief.
- The noise will continue for up to two minutes or until you unlock the device with your password.

Customize Lock Screen

- Locks your phone, the same as the Lock command, described above, and displays a text message on its panel.
- When you use this command, you might want to enter instructions for returning the phone, such as *If found, call 555-5555*.
- Available from the SecureAnywhere website only.

Using Lost Device Protection

For GSM-standard phones, the Premier/Complete versions of SecureAnywhere Mobile offers an additional feature that locks the phone if someone removes the SIM card. Your phone can only be unlocked with your password.

To disable the SIM Card Lock feature, go to Identity & Privacy from the main panel, and tap **Lost Device Protection** to see the SIM Card setting.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To use Lost Device Protection:

1. Make sure Lost Device Protection is enabled. To enable it from your device, tap **Identity & Privacy**, then tap **Lost Device Protection**. In the Lost Device Protection panel, the Device Protection setting displays an ON button.
2. If the button displays OFF, tap the button.
3. Another panel displays that instructs you to activate device administration. By activating administration, you are enabling enhanced Wipe command capabilities. If you initiate a Wipe, SecureAnywhere Mobile will perform a factory reset. Tap Activate in this panel.
4. Enter your Webroot account password.

   Note: If you can't remember your password, tap **Forgot Password** in the password dialog to receive a new password. This dialog opens for all Lost Device Protection functions

5. Once you activate Lost Device Protection, you can use the Lost Device commands from the SecureAnywhere website.

   Go to https://my.webrootanywhere.com and log in using your email address and Webroot password. For your device, click the **Lost Device Protection** tab, then select one of the commands in the panel.

   When you locate your phone, it displays a dialog with an option for unlocking your device using your password.

   - When you send a lock command from the portal, you will be asked to set a one-time-use PIN to unlock the device. On the device, instead of entering the uber password, you will now enter the one-

time PIN.

- When a lock command is sent, the PIN that goes with it will be logged in the portal. If the you forget the PIN that was sent, you can look in the device history to see the PIN.
- If you send a second lock command before unlocking the phone, the most recent PIN is the one you should enter to unlock it.

Note: If the lock command is being sent to an older version of this app, prior to 3.7.0.7170, you will not be asked for a PIN when you send the lock command; the app will work as it always has.

6. To view a list of commands sent, go to the Lost Device Protection panel in the SecureAnywhere Mobile app, then tap **Command Log**.

Chapter 6: Working With Threats

To work with threats, see the following topics:

Managing Ignored Threats

If you restored a threat from quarantine or chose to ignore it, SecureAnywhere Mobile adds the item to its Ignored Threats list. This list prevents SecureAnywhere Mobile from repeatedly detecting the same item in future scans. If you decide later that you want this item to be detected again, you can remove it from this list.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

To manage an ignored threat:

1. From the main SecureAnywhere Mobile panel, tap **Security** at the bottom.
2. Tap **Antivirus**.
3. Tap **More** at the bottom.
4. Tap **Ignored Threats**.
5. From the Ignored Threats panel, do either of the following:
   - To ignore just one threat, tap the threat name until another panel opens that gives you the option for removing the threat from the list.
   - To ignore all threats, press the **Menu** button for your mobile device, then tap **Clear Ignore List**.

Managing Quarantined Items

When you remove detected items, SecureAnywhere Mobile moves the files to quarantine, an area where files are rendered inoperable and can no longer run on your device. If you removed a detected item that you later decide you need, you can restore it to its original location. You can also permanently delete items from quarantine to conserve space on your device.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

This topic contains the following procedures:

- Viewing quarantined items
- Restoring or deleting quarantined items

To view quarantined items:

1. From the main SecureAnywhere Mobile panel, tap **Security** at the bottom.
2. Tap **Antivirus**.
3. Tap **Quarantine** at the bottom.

   The Quarantine panel displays the threat names and locations where they were found.

To restore or permanently delete quarantined items:

1. Tap the item name.

   Another panel opens with details about the item and options for restoring or deleting it. If your phone is set to disallow installation of applications from Unknown Sources, SecureAnywhere Mobile cannot restore the item until you disable the Unknown Sources setting. In this case, a message box provides instructions for restoring the application.

2. To delete multiple items, select the Menu button of your mobile device and tap **Clear Quarantine**.

   Note: Due to restrictions AT&T has placed on their Android phones, we cannot restore quarantined applications on AT&T phones. In this case, you must redownload the application from the Android Market.

Responding to Alerts

If SecureAnywhere Mobile detects a potential threat, it displays a red or yellow alert message on your device and in the SecureAnywhere website:

- A red exclamation displays for any threats that may pose a serious security risk or if your subscription has expired.
- A yellow exclamation displays for other items that are not serious, but may require your attention.

You can only fix an issue from your device app.

Note: WSA Internet Security Plus includes all features except Backup &Sync. For a comparison of products, see our product comparison for consumer products.

To respond to an alert:

1. Open the SecureAnywhere Mobile app. The main panel provides more information about the issue and provides options for fixing it.
2. Do one of the following:
   - If a Fix button displays, tap the button to resolve the issue.
   - If a threat was detected, SecureAnywhere Mobile gives you the option of removing it or ignoring it:
     - **Remove** — Your safest action is to remove the item. SecureAnywhere Mobile moves it to quarantine where it can no longer run on your device. You can restore it from quarantine later, if you decide that you need it. For more information, see *Managing Quarantined Items on page 28*.
     - **Ignore** — If you know the item is harmless, you can ignore it so SecureAnywhere Mobile will no longer detect the item during scans. For more information, see *Managing Ignored Threats on page 27*.

Enabling or Disabling Call & SMS Blocking Features

Call & SMS Blocking allows you to filter calls and text messages from undesirable or unknown sources. SMS, or Short Message Service, is the text communication service used for your mobile device.

Note: WSA Internet Security Plus includes all features except Backup and Sync. For a comparison of products, see our product comparison for consumer products.

Once you enter a phone number into the blocked list, calls from that number are sent directly to voicemail and text messages are simply blocked. If SecureAnywhere Mobile blocks a call or text, it displays a notification.

Note: The Call & SMS Blocking feature is not available on tablets without phone capabilities.

For added control over incoming calls and texts, Call & SMS Blocking includes these additional settings:

- **Block Unidentified Numbers** — Calls from unknown contacts are sent directly to voicemail. Texts from unknown contacts are blocked.
- **Block Malicious SMS** — Text messages that include a link to a malicious website are always blocked, even if the sender is a legitimate contact. Malicious websites might have viruses, malware, or phishing methods. If a text message includes a link to a suspicious website, one that could not be classified as malicious, but may contain threats, it allows the text to be received. If you click on the link, a yellow warning displays and allows you to decide if you want to proceed.

To disable or enable Call & SMS Blocking features:

1. From the main SecureAnywhere Mobile panel, tap **Identity & Privacy** from the bottom.
2. Tap **Call & SMS Blocking**.

   An ON button displays next to each feature if it is turned on.

3. Tap the button to turn the feature **ON** or **OFF**.

To create a blocked list:

1. From the Call & SMS Blocking panel, tap **Blocked Numbers** at the bottom.

   The panel displays any numbers you previously entered in the Blocked list.

2. To add a number or a short code that you want blocked, select the **Menu** button on your mobile device, then tap one of the following options:
   - **Add Number**
   - **Pick from Contacts**
   - **Pick from Call Log**
   - **Pick from Text Messages**

3. When you enter a number, make sure it includes all 10 digits, including the area code.
   - Once you place a number in the Blocked List, calls from that number are sent directly to voicemail.
   - Text messages are blocked. SecureAnywhere Mobile displays a message about the blocked call in the Notification bar at the top of your device.
   - Tap the message to get more information about the blocked message.

4. To view a log of all the calls and texts you have previously blocked, return to the Call & SMS Blocking panel and tap **Block Log**.

Chapter 7: WSA Mobile Security for Android Support

To learn more about Webroot's support options and other resources, see the following topics:

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Is your Webroot subscription through Best Buy? Click here for additional support options.
- Look for the answer in our knowledgebase and FAQs.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Security for Android forum.

Threat Analysis

If you are experiencing threat-related problems, you can collect log data and send it to a forum moderator for analysis.

To send log data for analysis:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. In the Settings panel, tap **General Settings**.
3. Tap **Support Options**.
4. Tap **Collect and mail logs**.
5. Contact a Webroot forum moderator for an email address where you can send the log file.

Force License Check

SecureAnywhere Mobile checks for changes to your subscription status every 24 hours. If you changed your subscription and want to refresh the license status immediately, use the following procedure.

To force a license check:

1. From the main SecureAnywhere Mobile panel, press your mobile device's **Menu** button.
2. In the Settings panel, tap **General Settings**.
3. Tap **Support Options**.
4. Tap **Force license check**.

Index

D

E

F

I

L

M