Activation & user guide

Set up ARMADA Antivirus 2.0.0 on Android, activate eligible access, and choose what to scan.

ARMADA ANTIVIRUS 2.0.0 / GOOGLE PLAY EDITION

Your setup at a glance

1. **Install the official app**
   Install ARMADA Antivirus from Google Play and connect your phone to the internet.
2. **Activate or restore access**
   Use the activation window when offered, the licence badge at the top right, or Settings > License & account. Review the Google Play offer before confirming a trial or subscription. Already subscribed? Restore access instead of buying again.
3. **Download signed definitions**
   Open Settings > Definitions and check for signed definitions. Wait for a verified package to become active.
4. **Choose your first scan**
   Open Scan and choose Start quick scan, Installed apps, or Files and folders. Grant only the access needed for your selected scope and review the result.
5. **Choose ongoing options**
   Enable Protection with separate consent, configure Scan schedule if wanted, or send an optional email summary after a scan.

Find the instructions you need

Section	Page
Activation, trial and subscription	2
AMDB definitions and updates	3
Scans, permissions and results	4
Protection and threat warnings	6
Scan schedule	8
Email scan summary	9
Restore and troubleshooting	10
Billing, privacy and support	11

English edition for ARMADA Antivirus 2.0.0 · Published 20 October 2026. Button labels refer to the English interface; Android screens may vary by phone.

Activate your licence

Signing in, checking eligibility and confirming a Google Play purchase are separate steps.

Licence badge or Settings > License & account

The first activation window

On the first launch, after a successful access check, eligible users without active access may see Start your 7-day trial. An active trial or licence does not need this prompt. Activate trial verifies your Google account and checks the available offer; signing in alone does not start a trial.

Not now does not start a timer

Not now closes the activation window without starting a trial or scheduling another automatic reminder. You can return through the licence badge or License & account. Attempting to scan without the required access can open activation again.

1. **Choose your account**
   Use Verify Google account and review the verification notice. Use Switch Google account if needed. The ARMADA account and the Google Play purchasing account may differ.
2. **Check the offer**
   Use Check trial availability in the activation window or Refresh subscription options in License & account. A new seven-day trial is offered only when eligible. Otherwise review the available annual subscription.
3. **Confirm deliberately in Google Play**
   Choose Start 7-day trial or the displayed subscription action. Review the purchasing account, localized price, payment method, trial end date and renewal terms on the Google Play purchase sheet before confirming.
4. **Verify active access**
   Return to the app and check the licence badge and License & account. Pending payment or an unverified purchase is not active access. Use Restore subscription and Refresh account status if the status is delayed; do not buy again to fix it.

If you already subscribed, use Already subscribed? Restore access or Restore subscription with the original accounts. Restore does not charge you or create another trial.

An eligible subscription trial lasts seven days and renews into the annual subscription unless cancelled before the deadline shown by Google Play. Without an eligible trial, the purchase sheet shows the applicable charge. If Founding 100 is offered, review its first-year and renewal prices; starting a trial alone is not completed paid membership.

Download the AMDB definitions

AMDB is the signed detection-definition database used by local ARMADA scans.

Settings > Definitions > Signed definitions

1. **Check access and connectivity**
   Confirm active licence access, a working internet connection and enough free storage.
2. **Request an update**
   Choose Check for signed definitions. Keep the app open while the first download and verification finish.
3. **Verify the active package**
   Look for Active and Signed package active. Release, Sequence and Last install identify the installed snapshot.
4. **Check freshness separately**
   Signed check records the last successful signed check. A successful check may confirm that the installed package is already the latest available; it does not always install a new package.
5. **Return to scanning**
   Once definitions are active, open Scan. You do not need to download an AMDB file from another website or import a supplied definition file.

Automatic update requests

The app requests automatic checks about every 12 hours and a foreground check when the last successful signed check is at least six hours old. Android may defer background work. Use the manual action to request a check and review the actual result.

If an update fails

Check connectivity, access and storage, then retry. A previously verified package may remain active after a failed update. Review both the active package and the last successful signed check; an active package alone does not establish freshness.

Unavailable definitions, blocked scans and update failures are not safe results. Resolve the problem before relying on a new scan.

Allow access & run a scan

Android controls which apps, files and folders ARMADA can read.

Home > Scan now or the Scan tab

Choose the scope

Action	Coverage
Start quick scan	Changed Android-visible user-app APK artifacts and the ARMADA app-controlled protected folder. It does not replace a broader check.
Installed apps	User and system base/split APK artifacts that Android makes visible and readable. Review the notice, then choose Start app scan.
Files and folders	Files or a folder selected with Android, or accessible shared storage when the separate access permission is enabled.

Allow notifications when requested, or review Settings > Notifications. For selected files and folders, use the Android picker and grant access only to the intended content. Broader shared-storage access has its own disclosure and Android permission; it does not expose another app's private data.

Review access through Settings > Privacy & access > Scanning & access, or Protection > Scanning & access. Optional all-files access is not a prerequisite for using the Android file picker.

Review the result

Manual and Daily scans take turns. If another scan owns the scanner, a manual request can show Waiting until the current Daily Scan finishes; a due Daily Scan waits for a running manual scan. Stop can cancel a waiting manual request. Waiting is not completed scanning, and valid access is checked when the queued scan actually starts.

Review Processed, Analyzed, Not analyzed and Detections. View details explains available findings, errors and coverage limits. No changed objects means this Quick Scan found nothing new to process; it is not a new full-device check.

If your licence expires during a scan

A scan admitted with valid access can finish if that access expires during the run. Review the retained result. If access is still inactive at completion, ARMADA shows a renewal notice; use Settings > License & account to renew or restore before starting a new scan. A notice is not a new entitlement. Android permission loss, Stop, process interruption and unavailable definitions can still prevent completion.

Allow access & run a scan

Continued

No threat detected is not a safety guarantee

No threat detected in scanned objects means no threat was identified in the successfully analyzed content with the active definitions. Unknown, inaccessible, skipped, interrupted or incomplete work remains unresolved. It does not certify every file or the whole phone safe.

Scan > Scan history shows recorded local activity. Export txt and Export json save the available report through your chosen destination. Quarantine creates a private vault copy when offered; it is distinct from deletion and does not automatically remove an original file or installed app.

Protection & threat warnings

Protection performs separately consented automatic local checks within Android-permitted scopes.

Settings > Protection or Home > Protection

1. **Enable Protection**
   Confirm active access and definitions. Choose Enable protection or Resume protection when shown, review the automatic-protection notice and confirm Agree and enable. Android-visible app APKs are the default automatic scope while Protection is enabled. Notification permission allows visible service and threat alerts.

2. **Choose one optional folder**
   Folder monitoring starts off. Use Choose or change monitored folder and grant Android read access to the intended local folder. Only one selected folder can be monitored; changing the selection replaces that scope. Android may restrict which folders are available. Your Daily Scan folder is selected separately.

3. **Enable folder monitoring deliberately**
   After selecting a folder, choose Enable folder monitoring. Selecting a folder alone does not turn monitoring on. If you choose Enable folder monitoring before selecting a folder, ARMADA opens the picker and enables that scope only after a valid selection. No Downloads, ARMADA protected folder or other file folder is included automatically.

4. **Review storage access only if needed**
   Review storage access opens the optional shared-storage explanation and Android access settings. Broad access alone neither selects a monitored folder nor turns folder monitoring on. The Android folder picker remains available without this optional permission.

5. **Review the actual state**
   MONITORING means supported observation is active; it does not prove that the last scan covered every object. Protection starting, Protection limited, Protection not running and Protection off are distinct states. Apps, Folder and Pending show current scope status; Off (optional) is expected when folder monitoring is disabled. Review incomplete checks and reasons in Scan history.

6. **Disable or remove the folder**
   Disable folder monitoring stops that optional scope but keeps your selection. Remove folder selection disables it and releases its Android read grant without deleting files. Leaving folder monitoring off does not itself make otherwise available Apps monitoring limited.

7. **Stop or resume deliberately**
   Turn protection off stops automatic monitoring. Resume protection requests it again when available. Normal phone-restart recovery is requested after unlock; Android controls whether and when it runs.

Protection & threat warnings

Continued

Threat warnings

Threat warnings is always available. With no retained automatic warning, its dialog reports that no warning is retained in this app session. When a warning exists, the button changes to Threat warning found — View details and opens the latest retained warning, including whether it was saved to History. Open app settings is offered for a known app when available.

The latest warning is process-local and may disappear after the app process ends; recorded History activity is separate and may contain aggregate counts rather than app details. An empty warning dialog does not establish that all content was checked or that the phone is safe.

Android limits still apply

Protection checks Android-visible app APKs and only the folder you explicitly select and enable. Downloads can be covered only when an eligible folder is selected and enabled; there is no default Downloads or automatic protected-folder scope. Android power management and provider events can delay work. Stop or Force stop can interrupt monitoring; ARMADA does not bypass your stop or provide continuous whole-device, private-app-data or kernel coverage.

Scan schedule & status messages

A saved schedule is a request for future work, not evidence that a scan completed.

Settings > Scan schedule

1. **Choose the scheduled scope**
   Select Selected folder and choose Select folder, or choose Shared storage and Allow storage access. Confirm the intended Android access. This scope is separate from the optional monitored Protection folder.
2. **Choose a daily time**
   Set Daily time, confirm active access and definitions, and allow notifications. Stop an unfinished scan before changing the scope or schedule.
3. **Enable and confirm**
   Choose Enable daily scan and review the schedule status. Retry daily scan request is available if a request was not confirmed; an unconfirmed request is not an enabled schedule.
4. **Review later activity**
   Check the recorded results and errors. Use Save changes to update an enabled schedule or Disable daily scan to stop future scheduled requests.

Manual and Daily content scans take turns rather than scanning simultaneously. A due Daily Scan waits for a running manual scan, and a manual request waits for an active Daily cycle, including a handoff between workers. A queued request needs valid access when it starts. Automatic Protection content work yields to these scans. Android power management or missing access can still delay or block a daily check; confirm actual completion in results or Scan history.

Temporary in-app messages

The bottom status line shows a temporary action or runtime message for five seconds. You can tap it for full text while it is visible; opening that temporary dialog does not extend its deadline. Its disappearance does not stop a scan, resolve an error or change a detection or incomplete result.

The licence badge, Protection coverage indicators, scan results and History remain separate from temporary messages. Android system protection notifications are also separate and may remain visible while the service runs. Use the i information buttons to open explanatory details where available.

Resume after phone restart
Enabled means ARMADA has requested automatic recovery after a normal restart and unlock. It does not ask you to restart the phone and does not guarantee that Android will start monitoring immediately.

Email scan summary

Send an optional aggregate report after a scan without opening an email app for normal server delivery.

Scan result or View details > Email scan summary

1. **Enter one recipient**
   Use Recipient email to enter the destination address. The Send button is immediately below the field; the keyboard's Done action is also available. No address is preselected for you.
2. **Review what will be sent**
   Read the short notice below Send or tap its i button. The server email contains aggregate scan statistics, not file names, paths, contents, ordinary-file hashes or an installed-app inventory. Sending also requests a current licence authorization check.
3. **Choose Send**
   The report is sent through ARMADA's service using support@acs.co.rs and mail.acs.co.rs. Normal sending stays on the scan screen; it does not require an email-composition popup or your phone's email app.
4. **Read the delivery result**
   Accepted by the mail server means SMTP acceptance, not confirmed delivery to the inbox. Check the recipient inbox and spam folder. A rejected or unauthorized request is not a sent report.

When the SMTP service is unavailable

Only a confirmed SMTP-unavailable result opens a popup asking whether to use your local email app. Choosing that option opens the existing text report in an email app, where you review and send it yourself. ARMADA never switches to this fallback or sends a second email automatically.

A phone connection timeout, authorization failure or uncertain submission does not prove that SMTP is offline, so it does not automatically open this popup. Follow the displayed retry or status controls. Do not repeatedly resend an uncertain request, because a first message may already have been accepted.

Temporary delivery messages disappear after five seconds; hiding them does not cancel a submitted email. The phone-client fallback may include more report detail than the server aggregate email. Review it before sending. ARMADA retains delivery metadata for up to 24 hours; the report and recipient are held in server memory only while sending. Mail providers and recipients may retain the email. See the Privacy Policy for details.

Restore access & solve setup problems

Use your original accounts after reinstalling and avoid duplicate purchases.

1. **Install from Google Play again**
   Choose the Google Play account holding the subscription. In Settings > License & account, verify the account originally used for ARMADA.
2. **Restore the existing purchase**
   Choose Restore subscription and review the status. Use Refresh account status if needed. Follow Link existing purchase only when offered; restoring is not a new purchase.
3. **Review local setup separately**
   Check definitions, file and notification access, Protection and Scan schedule. Restored billing does not guarantee that local settings, History or Vault contents have been restored.

A reinstall does not reset a trial
If Recover original trial remainder is offered, it recovers only the original interval still remaining on the first qualifying phone. It does not start another seven days or transfer that trial to another phone. A reset or Android-profile change may affect recovery.

Common problems

What you see	What to do
Paid in Play, access inactive	Check both accounts, restore and refresh. Review pending payment or billing issues in Google Play; contact support if access remains missing.
No trial or offer	Refresh offers and verify the selected account and eligibility. Do not assume every account or phone qualifies for a new trial.
Definitions unavailable	Check licence access, connection and storage; retry the signed-definition action.
Scan incomplete or disabled	Review definitions, access, running scans and not-analyzed items. A blocked scan is not a safe result.
Protection starting or limited	Review Apps, Folder, Pending, any enabled folder read grant, definitions and Android background restrictions. MONITORING describes active observation; review Scan history for incomplete checks. Folder Off (optional) is expected unless you selected and enabled that scope.
Email not received	Check acceptance status, inbox and spam. Authorization and phone-connectivity errors are different from confirmed SMTP unavailability.

Switching the ARMADA account does not switch Google Play's billing account or cancel renewal. A purchase already linked to another ARMADA account is not automatically transferred.

Billing, privacy & support

Keep your purchase receipt and use the account that holds the subscription.

Manage or cancel renewal

Open Settings > License & account > Manage subscription. Alternatively, in Google Play select the purchasing account, then Payments & subscriptions > Subscriptions > ARMADA Antivirus. Review the next billing date, renewal price and payment method.

To avoid the first paid charge after an eligible trial, cancel before the deadline shown in Google Play and check the cancellation confirmation. Access follows the period and status reported by Google Play and ARMADA.

Uninstalling is not cancellation
Uninstalling ARMADA, signing out or requesting account-data deletion does not cancel Google Play billing. Manage renewal separately in Google Play.

Your files and account data

Scanning takes place on your phone. The default scan flow does not upload scan files, paths, item details or Vault contents. Account verification, licensing and definition updates use online services. Optional email sends the recipient and aggregate report only when you choose Send; the separate email-app fallback shares the existing text report with the app you select.

Read the Privacy Policy

Contact ARMADA support

support@acs.co.rs

Include the phone model, Android version, ARMADA version from Settings > About ARMADA, the time and exact error, and relevant licence or definition status. For a purchase issue, send the Google Play order reference and the ARMADA account reference if available.

Send account or order references directly to support, not publicly. Never send passwords, payment-card details, licence tokens or suspicious files.

Useful links

ARMADA Antivirus on Google Play

Google Play subscription-management help

Setup is complete when access and signed definitions are active and you have reviewed the first scan. If you enabled Protection or Scan schedule, check their actual coverage and execution separately.