ESET Endpoint Security for Android FAQ (2.x)

Ondersteuning | ESET Nederland - 2017-12-04 - Reacties (0) - ESET Endpoint Security Android

https://support.eset.com/kb3619

Issue

Frequently asked questions for ESET Endpoint Security for Android version 2.x
ESET Endpoint Security for Android version 2.x replaces version 1.x and is designed to be used with version 6 ESET business products (it is equivalent to version 6 business products).

Details

Solution

Are you a Home user?

What's new in EESA 2.x | Known Issues (opens in new window) | System Requirements | Download/Install | Use with ESET Remote Administrator | Privacy Policy for App permissions

---

ESET Endpoint Security for Android protects your business from malware infections, intercepts unwanted phone calls and filters SMS/MMS spam to minimize risk of data loss. It enables your IT manager to remotely monitor and control the security level of your Android smartphones/tablets, without the cost and complexity of a Mobile Device Management solution.

1. **What is ESET Endpoint Security for Android?**
   ESET Endpoint Security for Android protects your business from malware infections, intercepts unwanted phone calls and filters

SMS/MMS spam to minimize risk of data loss. It enables your IT manager to remotely monitor and control the security level of your Android smartphones/tablets, without the cost and complexity of a Mobile Device Management solution.

2. **Why do I need ESET Endpoint Security for Android?**
   ESET Endpoint Security for Android is useful for:

   - Businesses that share files between their mobile devices and workstations
   - Businesses that need the ability to protect mobile devices in the event that they are lost or stolen
   - Businesses that are subject to regulatory compliance requirements to protect all endpoints including mobile devices with antivirus solutions installed

3. **What are the key features included in ESET Endpoint Security for Android 2.x?**

   - **Hide license expiration (version 2.0.142 and later)**—Ability for the ERA administrator to hide license expiration status on endpoints
   - **Application Control**—An added layer of security to protect against rogue applications by providing administrators with the option to monitor installed applications, define those to be blocked by specific criteria and prompt users to uninstall them.
   - **Device Security**—Allows administrators to execute basic security policies across a mobile device fleet, and achieve compliance with corporate security policies (such as setting the complexity of screen lock codes, maximum number of failed unlock attempts, lock screen timer and the ability to restrict camera usage).
   - **Anti-phishing**—Protects users from attempts by fake websites to acquire passwords, banking data and other sensitive information.
   - **Improved Anti-Theft**—Minimize data loss and trigger remote commands via ESET Remote Administrator 6, SMS or directly from the admin’s product interface (useful for companies that do not use remote management, or when the admin is out of the office).

- **Import/Export of settings**—If mobile devices are not managed via ESET Remote Administrator, an admin can share settings from one mobile device to another by exporting them to a file and importing the file to any device running the client application.
- **Notification center**—Provides users with one unified notification center where they can find all notifications regarding application features that require their attention. Notifications are organized according to priority, with higher priority notifications displayed at the top of the list.
- **Background scanning**—On-Demand Scanning provides reliable scanning and cleaning of integrated memory and exchangeable media. The scan runs in the background and can be paused by the user or scheduled to run at a specific time.
- **Time-based rules for SMS & Call filter**—This protects users from unwanted calls and SMS messages during pre-defined time periods from hidden numbers and selected contacts or phone numbers.
- **New Licensing System**—The ESET License Administrator portal allows administrators to manage credentials for their software, convert older Username and Password based credentials into License keys for use with ERA 6 and grant license management privileges to co-workers or partners. For more information, see the ESET License Administrator User Guide.
- **Improved Device Enrollment**—During the enrollment process, mobile devices are whitelisted so only authorized devices can connect to ESET Remote Administrator. This simplifies individual device identification − by name, description and IMEI.
- **Display message from ERA**—When managing devices remotely, the administrator can send a custom message (pop-up) to a particular device or a group of devices.

4. **What are the system requirements and recommended system configuration?**

    - Nougat (7.0)

- Marshmallow (6.0) (see known issues)
  Lollipop (5.0–5.1.1)
  KitKat (4.4–4.4.4)
  Jelly Bean (4.1–4.3.1)
  Ice Cream Sandwich (4.0–4.0.4)
  (Remote Wipe and Uninstall protection available on Android 2.2 and higher)
- A 600+ Mhz processor
- 20 MB free storage space
- A touch screen with resolution 480 x 800 px
- CPU: ARM with ARMv7 instruction
- An internet connection is required for updates to function properly (Wi-Fi or Cellular Data)

5. **How do I install and activate ESET Endpoint Security for Android 2.x?**

   - For instructions on installing ESET Mobile Security for Android using ESET Remote Administrator, see the following ESET Knowledgebase article:

     How do I deploy ESET Endpoint Security for Android (2.x) using ESET Remote Administrator? (6.x)

   - For instructions on installing ESET Mobile Security for Android manually, see the following ESET Knowledgebase article:

     How do I install ESET Endpoint Security for Android? (2.x)

6. **Can ESET Endpoint Security for Android be used with ESET Remote Administrator?**
   Yes. Mobile devices running ESET Endpoint Security for Android version 2.x can be managed locally or remotely using ESET Remote Administrator version 6.x and later. While it may appear that you can manage ESET Endpoint Security for Android clients using earlier versions of ERA, attempting to do so may result in errors and is not recommended.

7. **Does ESET Endpoint Security for Android protect against SMS spam and MMS email?**
   ESET Endpoint Security for Android offers SMS/MMS spam filtering using a Whitelist and Blacklist. The integrated On-access scanner protects against malicious email attachments.

8. **How does ESET Endpoint Security for Android receive virus signature database updates?**
   ESET Endpoint Security for Android downloads updates over the internet. From the main menu tap **Antivirus → Update → Virus signature database** to manually check for virus signature database updates. ESET Endpoint Security for Android will automatically check for virus signature database updates every day using default settings, but you can increase the frequency to six hours.

9. **How big are virus signature database updates?**
   Updates are designed to be small for the convenience of users who have slow or limited internet access. The current update file is under 1000 bytes. We anticipate 20 to 40 bytes of increase in update size for each new threat added.

10. **Which languages are available?**
    The application and the related documentation is available in 29 languages.

11. **Who pays for downloading updates?**
    You are responsible for all costs associated with downloading virus signature database updates (for example, data transmission and roaming fees).

12. **Which browsers are protected against Phishing?**
    In general, Anti-Phishing protection is available for stock browsers that come as pre-installed on Android devices.

Privacy Policy for App permissions

ESET does not use these permissions for data collection or marketing purposes. To protect your personal information and your Android device’s resources, ESET Endpoint Security for Android must first have access to your device functions and in some cases control over them.

For detailed explanations of what each type of permission is used for, see the table below.

Permission settings for Android 6 (Marshmallow)

If you receive the message "Screen overlay detected" after granting permissions in your ESET mobile product for Android, see our Knowledgebase article to resolve the issue.

To see the permissions given to ESET Endpoint Security for Android after installation, follow the steps below:

1. Tap **Settings → Apps** (or **Manage Applications**) to open your device (in some cases, tap **Menu → Settings**).

2. Tap **ESET Endpoint Security** to view the application's specific permissions.

For Anti-Phishing to function properly and protect you against dangerous web sites, you must allow the **Accessibility** permission.

Permissions for Android version 4 and 5

App permission title	Google Play description	Mobile Security & Antivirus usage
In-app purchases	Allows the user to make purchases from within the app	ESET Endpoint Security does not allow in-app purchases
Device & app history	Accesses information about device activity, apps that are running, browsing history and bookmarks	• Allows access to your web browser history and bookmarks so that the Wipe command can be used to delete this data from your device in the event it is marked missing. • Anti-Phishing analyzes URLs in your browsing history to determine if they are unsafe and to protect against malicious websites attempting to acquire your sensitive information. • Allows administrator to block applications.
Identity	Accesses accounts and profile data on the device	• Accesses basic user data so you can sign in to your accounts. • Allows the Remote Wipe command to remove personal accounts from your device if you activate the Wipe command.
Calendar	Accesses calendar information	Allows access to the calendar so that it can be deleted from your device if you activate the Wipe command.
Contacts	Accesses contact information	Allows contacts to be added from contact list. Used by the Anti-Theft and Anti-Spam features.
Location	Accesses device location	Retrieves the location of your device when you request the location from an authorized device or ESET Remote Administrator server.
SMS	Accesses SMS and MMS; charges may apply.	• Allows access to your MMS and SMS logs for the SMS Filter feature and the block text messages feature. • ESET Mobile Security monitors for SMS commands such as the lost password command. • Notifies administrator about missing trusted SIM card.
Phone	Accesses phone and call log. Charges may apply.	Accesses your phone settings for the Call Filter, Group Blocking and Block Last Caller features to be able to block incoming calls from blocked contacts that you have set. Modifies the audio settings to increase the device volume if you use the Siren command.
Photos/Media/Files	Accesses device files, (images, videos, audio or external storage)	Allows ESET Endpoint Security to access your files and search for threats to keep your device safe. Allows access for the Wipe command in the event that the device is stolen.
Camera	Accesses device camera(s)	Allows administrator to restrict camera usage.
Wi-Fi connection information	Accesses information about Wi-Fi networking, Wi-fi usage, and connected Wi-Fi device names	• Checks online status when Anti-Theft commands are sent (Lock, Find, Siren, and Wipe) and allows device to update virus database. • Sends information to ESET Remote Administrator server. • Receives information and updates from ESET Remote Administrator server.

Device ID & call information	Accesses phone number and device IDs, call activity, and the remote number connected by a call.	• Allows the unique device identifier to connect or reconnect the device to your my.eset.com account. • Accesses your phone settings for the Call Filter, Group Blocking and Block Last Caller features to be able to block incoming calls from blocked contacts that you have set. Modifies the audio settings to increase the device volume if you use the Siren command.

Permissions for Android version 6 and later

ESET Mobile Security uses dynamic permissions for Android version 6 and later. You will be asked to allow application permissions the first time you use the application features requiring those permissions.

Application feature	App Permission title	Mobile Security & Antivirus usage
Installation	Phone	• Links the license to the unique device identifier to activate the product. • Allows phone information to be sent to ESET Remote Administrator server.
	Storage	• Accesses your files and searches for threats to keep your device safe • Allows ESET Remote Administrator to manage the application
Antivirus	Storage	Accesses your files and searches for threats to keep your device safe.
SMS and Call Filter	SMS	Stops unwanted calls and messages.
	Phone	Stops unwanted calls and messages.
Anti-phishing	Accessibility	Analyzes URLs in your browsing history to determine if they are unsafe and to protect against malicious websites.
Anti-Theft	Location	Retrieves the location of your device when you request the location from an authorized device or ESET Remote Administrator server.
	SMS	Accesses SMS commands in the event the device is lost or stolen.
	Phone	Identifies the SIM Card.
Draw over other apps		Necessary for Anti-Theft to be able to lock the device in the event that your device is stolen. (If you download ESET Endpoint Security from Google Play, this permission is activated by default)

- Tags
- Android