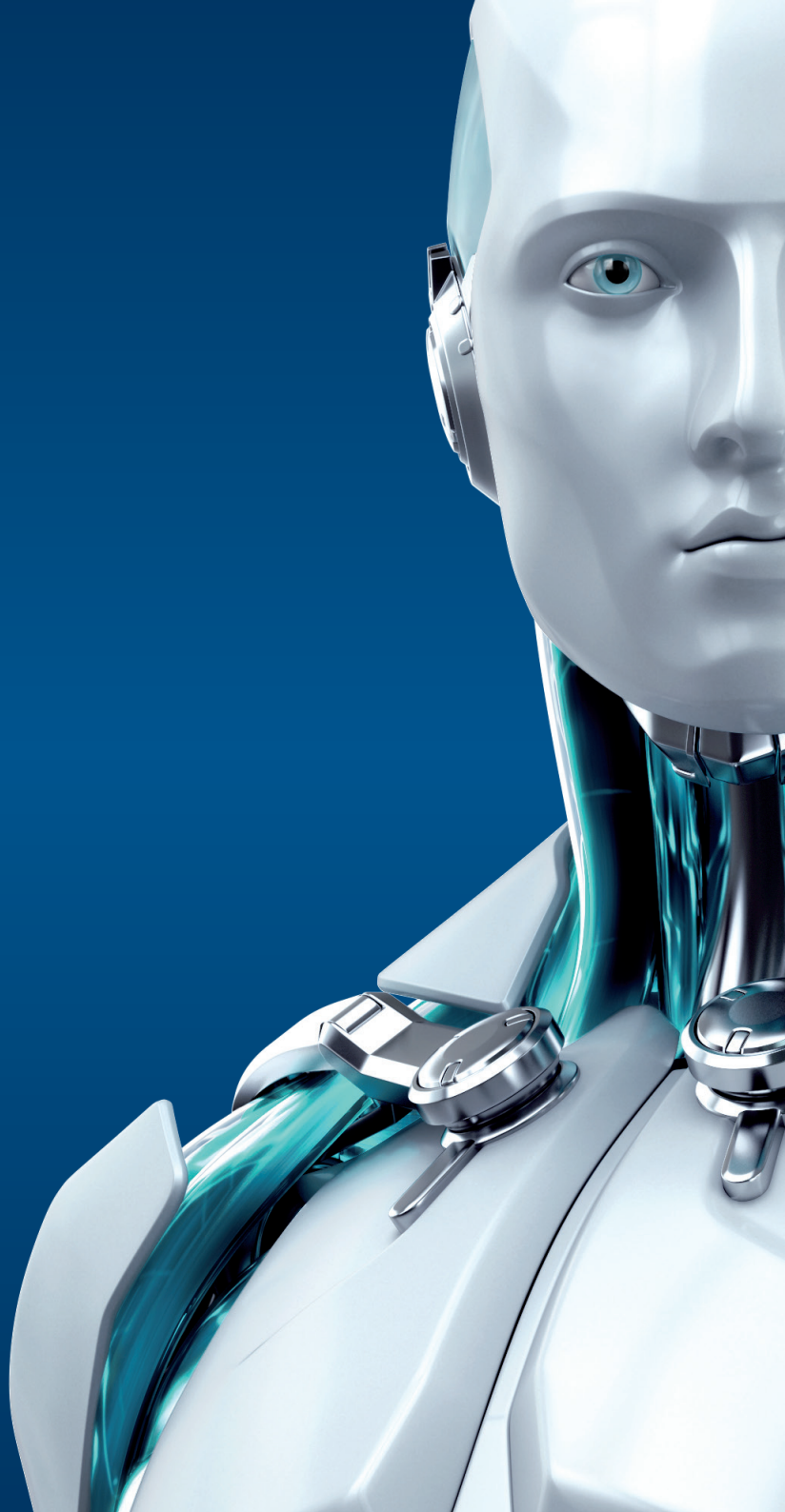
ENDPOINT SECURITY
FOR ANDROID

ENJOY SAFER TECHNOLOGY™



ENDPOINT SECURITY
FOR ANDROID

ESET Endpoint Security for Android protects your company's mobile fleet with ESET NOD32® proactive technology.

It scans all applications, files and memory cards for malware. The Anti-Theft system protects the physical devices, which can be remotely locked or wiped if they are lost or stolen. Users are spared unwanted calls and SMS messages, and administrators can push security policies to all devices to ensure compliance.

Endpoint Protection

Real-time Protection	Shields all applications and files in real time using ESET NOD32® proactive technology, optimized for mobile platforms. The integrated ESET LiveGrid® malware collection system, in conjunction with advanced scanning, protects company smartphones and tablets from threats.
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 user. It is also possible to schedule the exact time to run a scan.
On-Charge Scan	Allows a full scan to be conducted during off-peak hours when the device is being charged and the screen is locked.
Anti-Phishing	Protects users from attempts by fake websites to acquire passwords, banking data and other sensitive information.
Uninstall Protection	Prevents the app from being uninstalled without an administrator password.
SMS & Call Filter	Protects users from unwanted calls and SMS messages* from hidden numbers, selected contacts or phone number, or during pre-defined time periods.
	*Due to changes in Android OS made by Google (from version 4.4 Kitkat) the SMS blocking functionality will be not available.

Device Security

Provides the administrator with options to execute basic security policies across the mobile device fleet. The application automatically notifies user and admin if the current device settings are not in compliance with corporate security policies and suggests changes to settings to comply.

Device Security Settings	Define password complexity requirements Set maximum unlock attempts after which the device will automatically go to factory settings Set maximum screen lock code age Set lock screen timer Prompt users to encrypt their mobile devices Block built-in camera usage

Device settings policy – allows admin to monitor pre-defined device settings to determine if they are in compliance. Admin can oversee memory usage, Wi-Fi connection, data roaming, call roaming, unknown sources - other than Google Play store, USB debug mode, NFC, Internal Storage Encryption and their current state.

Anti-Theft

Command Triggers	All the remote commands can be triggered by admin via ESET Remote Administrator, via an SMS with two-factor verification code, or directly from the admin's product interface - especially useful for companies not using remote management or when admin is out of office.
Remote Lock	Locks lost or stolen devices remotely. After locking, no unauthorized person can access the data stored on the device. Once the device is found/returned, a remote unlock command unlocks the device for use.
Remote Localization	Remotely locates the phone and tracks its GPS coordinates.
Remote Wipe	Safely deletes all contacts, messages and data stored in the device's internal memory, as well as on the removable memory cards. Advanced cleaning procedures ensure that it is not be possible to restore the wiped data. After the remote wipe, ESET Endpoint Security for Android remains installed on the device, so it is possible to execute any other Anti-Theft command.
Remote Siren	When activated, a siren is sounded on the device, even if the volume is set to mute. Simultaneously, the missing device is locked automatically.
Remote Factory Reset	Removes all accessible data on the device by destroying the file headers and resetting the device to its factory settings.
Custom Message	Administrator can send a custom message to a particular device or to a group of devices. The message will be displayed in the form of a pop-up, so the user will not overlook it.
Lock Screen Information	Administrator is able to define custom information (company name, email address, message) to be displayed even when the phone is locked. This enables a potential finder to call a pre-defined number.
Trusted SIM	When an unauthorized SIM card is inserted, the device is automatically locked, with information about it sent to administrator.
Admin Contacts	Contains a list of administrator phone numbers protected by administrator password. SMS commands to control the devices can be sent only from these trusted numbers. In addition, these numbers are used for notifications related to Anti-Theft actions.

FREE LOCAL TECHNICAL SUPPORT

Do More with the help of our specialists. On call to provide technical support when you need it, in your language.

Application Control

Offers administrators the option to monitor installed applications, block access to defined applications, and prompt users to uninstall particular applications.

Application Control Settings	Manually define applications to be blocked. Category-based blocking - e.g. games, social media, etc. Permission-based blocking - e.g. applications that track location, access contact lists, etc. Blocking by source - applications installed from sources other than default app stores. Set exceptions from the rules for blocked applications – whitelist application. Set a list of mandatory installed applications.
Application Audit	Tracks applications and their access to personal/company data sorted by categories, allowing administrator to monitor and control applications' access.

Usability and Management

Import/Export Settings	If mobile devices are not managed via ESET Remote Administrator, admin can easily 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	User can access all notifications which require attention in one place, together with information on how to solve the issue. This makes it easier for user to be compliant with company policies.
Local Administration	Admin can set up and manage the device locally if the company doesn't use ESET Remote Administrator. All application settings are protected by administrator password, keeping the application under full administrator control at all times.
Improved Device Identification	During the enrollment process, mobiles are whitelisted so only authorized devices can connect to ESET Remote Administrator. This simplifies individual device identification – by name, description, and IMEI.
Set-up Wizards	Post-installation setup wizards are available for selected features, streamlining the whole process when the device settings are implemented locally.
Remote management	ESET Endpoints are fully manageable via ESET Remote Administrator. Deploy, run tasks, set up policies, collect logs, and get notifications and an overall security overview of your network – all via a single web-based management console.
ESET License Administrator	Lets you handle all licenses transparently, from one place via web browser. You can merge, delegate and manage all licenses centrally in real-time, even if you are not using ESET Remote Administrator.