ESET

ENDPOINT SECURITY
FOR ANDROID

Protect your company's Android mobile fleet with ESET NOD32® proactive technology. The integrated ESET LiveGrid® malware collection system, in conjunction with advanced scanning, protects company smartphones and tablets from threats. The application automatically notifies user and admin if the current device settings are not in compliance with corporate security policies and suggests changes.

GET IT ON Google play

Mobile Device Management for Android

Device settings policy	ESET Endpoint Security for Android allows admins to monitor pre-defined device settings to determine if they are in compliance. The admin can monitor memory usage, Wi-Fi connection, data roaming, call roaming, unknown sources – other than Google Play store – USB debug mode, NFC and internal storage encryption, and their current states. All the remote commands can be triggered by the admin via ESET Remote Administrator or via an SMS with two-factor verification.
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.
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 applications. • Set a list of mandatory installed applications.
Application audit	Track, monitor and control applications and their access to personal/company data, sorted by categories.
Anti-Theft protection	Remotely lock/unlock devices, wipe all the data they hold in the event they are lost or stolen, or locate the phone and track its GPS coordinates. Remove all accessible data on the device by destroying the file headers and resetting the device to its factory settings.
Custom message	Admins can send a custom message to a particular device or to a group of devices. The message is displayed in the form of a pop-up, so the user does not overlook it.
Remote management	ESET-secured 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	Handle all licenses transparently, from one place, via web browser. Merge, delegate and manage all licenses centrally in real-time, even if not using ESET Remote Administrator.

Copyright © 1992 – 2017 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2008.

MOBILE DEVICE MANAGEMENT
FOR APPLE iOS

Integration of Apple iOS MDM framework in ESET Remote Administrator allows you to configure security-related iOS device settings from a single point, as with other ESET Security products, without the need for an app to be installed on each iOS device. You can enroll both iPhones and iPads and set up security profiles on them that will allow you to adjust their security settings, including Anti-Theft, settings for Exchange, Wi-Fi, and VPN accounts, Passcode, iCloud and others. Admins can also white/black-list apps and enforce web filtering to block prohibited content.

Mobile Device Management for Apple iOS

Device Enrollment Program	Apple devices belonging to customers who are members of Apple's Volume Purchase Program (VPP) can automatically participate in our Device Enrollment Program. Such devices are fully manageable and allow multiple, granular policies and settings to be applied, for example initial configuration of the device, app removal, automatic app downloads, and blocking/allowing radio, music services or Game Center.
App white/black listing & notifications	Create white/black lists of apps to prevent users from installing prohibited apps. Also manage app notifications to users, including options for Notification Center, Sounds, Badge App Icon and others.
Web content filtering	Adult web content, as defined by Apple, can be blocked. The admin can also white/black-list specific URLs.
Push account setttings remotely	Remotely push out account settings to iOS devices in batches – for the Exchange, Wi-Fi, and VPN accounts.
Manage device settings remotely	Significantly increase the security of your company's iOS devices by remotely pushing out security settings and restrictions of Passcode, iCloud, Privacy and others.
Anti-Theft protection	Remotely lock/unlock devices or wipe all the data they hold in case they are lost or stolen.
Remote management	ESET Mobile Device Management for Apple iOS comes integrated within ESET Remote Administrator, giving you a single point of overview of network security, including all endpoints, mobiles & tablets (iOS, Andorid) and servers.
Cost effective	No need for dedicated solutions – take advantage of Apple iOS Management Framework and oversee security of all company iOS devices – from a single point with ESET Remote Administrator 6.
Simple licensing	Mix and match your license seats exactly as you need. Migrate seats from one device to another, regardless of the OS. For example, you can move the license seat from ESET Endpoint Security for Android to ESET Mobile Device Management for Apple iOS and vice versa.
Prerequisites	• ESET Remote Administrator 6.3 and newer • ESET MDM Core (ESET Remote Administrator Mobile Device Connector) • Company Apple iTunes ID • Valid ESET license • iOS devices running on iOS 8+ (iPhone and iPad)

Copyright © 1992 – 2017 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2008.