



ENDPOINT SECURITY FOR ANDROID

Chroń urządzenia mobilne z systemem Android dzięki aktywnej technologii ESET NOD32®. Zintegrowane oprogramowanie antywirusowe ESET LiveGrid skanuje wszystkie pliki, aplikacje i karty pamięci w poszukiwaniu złośliwego oprogramowania na Twoich urządzeniach mobilnych. Jeżeli ustawienia urządzeń mobilnych są niezgodne z polityką bezpieczeństwa nadaną przez administratora - aplikacja od razu powiadamia o tym fakcie użytkownika i administratora proponując zmiany.



Mobile Device Management dla systemu Android

Polityka ustawień urządzenia	ESET Endpoint Security for Android umożliwia administratorom monitorowanie predefiniowanych ustawień urządzenia, aby sprawdzić ich tryb zgodności. Administrator może monitorować wykorzystanie pamięci, połączenia WiFi, dane roamingu, nieznanne źródła – inne niż sklep Google Play – tryb debugowania USB, NFC i szyfrowanie pamięci wewnętrznej. Wszystkie komendy mogą być wyzwalane przez administratora za pośrednictwem ESET Remote Administrator lub poprzez SMS z dwuetapową weryfikacją.
Zabezpieczenia urządzenia	<ul style="list-style-type: none">• Zdefiniuj wymagania złożoności hasła• Ustaw maksymalną liczbę nieudanych prób odblokowania urządzenia, po której urządzenie automatycznie zostanie przywrócone do ustawień fabrycznych• Ustaw maksymalny czas ważności kodu blokującego urządzenie• Ustaw czas po jakim ekran zostanie automatycznie zablokowany• Zasugeruj użytkownikowi szyfrowanie swojego urządzenia• Zablokuj możliwość korzystania z wbudowanej kamery
Ustawienia kontroli aplikacji	<ul style="list-style-type: none">• Zdefiniowanie, które aplikacje powinny być blokowane:<ul style="list-style-type: none">• Blokowanie aplikacji według kategorii - gry, media społecznościowe• Blokowanie aplikacji według dostępu do konkretnych danych, np. wymagających dostępu do danych lokalizacji urządzenia lub dostępu do listy kontaktów• Blokowanie aplikacji według źródła pochodzenia, np. pochodzące z innego miejsca niż Google Play• Ustawienie wyjątków od reguł - biała lista aplikacji dozwolonych• Zdefiniowanie listy obowiązkowych dla danego pracownika aplikacji
Kontrola aplikacji	Sprawdza, które aplikacje żądają dostępu do konkretnych kategorii danych, co pozwala na ich kontrolę przez administratora.
Anti-Theft - ochrona przed kradzieżą	W razie kradzieży lub zgubienia urządzenia skorzystaj z Anti-Theft - i zdalnie usuń dane z urządzenia przywracając urządzenie do ustawień fabrycznych.
Wysyłanie powiadomień	Administrator może wysłać niestandardową wiadomość do danego urządzenia lub grupy urządzeń. Wiadomość zostanie wyświetlona w formie pop-up, więc użytkownik nie przeoczy jej.
Zdalne zarządzanie	Programem ESET dla urządzeń mobilnych można w pełni zarządzać za pomocą ESET Remote Administrator. Wdrażanie, uruchamianie zadań, ustanawianie polityk, zbieranie logów, otrzymywanie powiadomień i ogólny przegląd zabezpieczeń sieci - wszystko za pomocą nowej webowej konsoli zarządzającej.
ESET License Administrator	ESET License Administrator zapewnia jeszcze bardziej przejrzysty widok statusów posiadanych licencji i ich wykorzystywania w czasie rzeczywistym, nawet bez podłączenia do ESET Remote Administrator.



MOBILE DEVICE MANAGEMENT FOR APPLE iOS

Dzięki integracji Apple iOS MDM Framework z konsolą ESET Remote Administrator (od wersji 6.3) możesz konfigurować zabezpieczenia urządzeń Apple z poziomu jednej konsoli ESET. Nie musisz instalować żadnych dodatkowych aplikacji, wystarczy licencja dla rozwiązania ESET i konsola ESET Remote Administrator by zarządzać bezpieczeństwem firmowych iPhone'ów i iPadów. Konfiguruj zdalnie pocztę (Exchange), wymagaj ustawień haseł, zarządzaj polityką iCloud, konfiguruj klientów VPN'owych, itp. Ponadto administratorzy mogą również tworzyć listy dozwolonych i/lub zabronionych aplikacji oraz ustawić filtrowanie dozwolonych stron internetowych.

Mobile Device Management for Apple iOS

Device Enrollment Program	Urządzenia firmy Apple, należące do klientów będących członkami Apple's Volume Purchase Program (VPP) mogą automatycznie uczestniczyć w Programie Device Enrollment firmy ESET. Takie urządzenia mogą być w pełni konfigurowane i pozwalają na szczegółowe określenie polityk bezpieczeństwa. Dzięki temu możliwe jest m.in. wstępne skonfigurowanie urządzenia, usuwanie aplikacji lub automatyczne ich pobieranie, a także blokowanie i/lub udostępnianie możliwości słuchania radia czy korzystania z innych serwisów muzycznych czy centrów gier.
Białe/czarne listy aplikacji	Twórz listy aplikacji, które są dozwolone lub zabronione, dzięki czemu zezwolisz lub uniemożliwisz użytkownikom instalowanie konkretnych aplikacji. Możesz także zarządzać powiadomieniami aplikacji z centrum powiadomień, powiadomieniami dźwiękowymi oraz powiadomieniami wyświetlanymi przy ikonach programów.
Filtrowanie stron internetowych	Niektóre, zdefiniowane przez firmę Apple, kategorie stron internetowych mogą być blokowanie automatycznie np. strony zawierające treści przeznaczone dla osób dorosłych. Dodatkowo możesz sam dodać konkretne adresy URL, które powinny być blokowane lub udostępnianie pracownikom Twojej firmy.
Zdalna konfiguracja	Zdalnie konfiguruj ustawienia poczty (MS Exchange) na danym urządzeniu iOS, konfiguruj klienty VPN oraz ustawienia sieci WiFi.
Zdalne zarządzanie ustawieniami urządzeń	Poprzez zarządzanie kodami odblokowującymi, iCloud, ustawienia prywatności i ustawienia urządzenia, a także zarządzanie ograniczeniami, możesz w znaczący sposób zwiększyć bezpieczeństwo firmowych urządzeń z systemem iOS.
Anti-Theft	W razie kradzieży lub zgubienia urządzenia masz możliwość zablokowania urządzenia, zdalnego przywrócenia ustawień fabrycznych czy zlokalizowania urządzenia na mapie Google.
Zdalne zarządzanie	ESET Mobile Device Management dla urządzeń z iOS jest zintegrowane z ESET Remote Administrator (od wersji 6.3), dzięki czemu możesz zarządzać wszystkimi urządzeniami w swojej sieci, w tym stacjami roboczymi, serwerami i urządzeniami mobilnymi.
Uzasadnione ekonomicznie	Brak konieczności zakupu dodatkowych narzędzi – zarządzaj wszystkimi urządzeniami firmowymi z systemem iOS dzięki ESET Remote Administrator w wersji 6.
Proste licencjonowanie	Mieszaj i paruj swoje licencje, dopasowując je do swoich potrzeb. Migruj licencję z jednego urządzenia na inne, bez względu na system operacyjny.
Wymagania systemowe	<ul style="list-style-type: none">• Posiadanie aktywnej licencji dla rozwiązania ESET Endpoint Security• ESET Remote Administrator w wersji 6.3 lub nowszej• ESET MDM Core (ESET Remote Administrator Mobile Device Connector)• Firmowe ID w usłudze iTunes firmy Apple• Urządzenia z systemem iOS działające na iOS 8+ (iPhone i iPad)