COMODO IT & Security Manager

ABC konsoli w chmurze

COMODO
Creating Trust Online™

Tel +48 (32) 745 46 01
NIP 634 280 10 31
KRS 0000403252
SĄD REJONOWY KATOWICE-WSCHÓD,
VIII WYDZIAŁ GOSPODARCZY KRAJOWEGO
BANK ZACHODNI 39 1090 2008 0000 0001 1771 9659

COMODO Polska
it partners security sp.z o.o.
wyłączny dystrybutor na
Polskę, Czechy, Litwę i Węgry
ul. Paderewskiego 35
40-282 Katowice Poland
Email: biuro@comodo-polska.pl

Spis treści

Wstęp

Producent COMODO, wychodząc naprzeciw zapotrzebowaniu współczesnych firm na kompleksowe monitorowanie i zarządzenie urządzeniami niezależnie od systemu operacyjnego, opracował produkt COMODO IT & Security Manager, który może być wdrożony w każdej firmie niezależnie od jej wielkości.

Rozwiązanie z dostępem do konsoli w chmurze oferuje administratorom bezproblemowe monitorowanie stanu bezpieczeństwa urządzeń wykorzystywanych do pracy. Komputery z systemem Windows mogą być dodatkowo zabezpieczone przed złośliwymi aplikacjami i zagrożeniami 0-day przez znane i doceniane na całym świecie oprogramowanie Comodo Endpoint Security.

W skład pakietu ochrony wchodzą:

Agent konsoli

ITSM Agent *(COMODO IT & Security Manager Agent) – to lekki agent instalowany na urządzeniach z systemem Windows, Android, iOS, którego zadaniem jest powiązanie urządzenia z konsolą w celu przekazywania informacji o stacji oraz respektowanie skonfigurowanych w konsoli profili bezpieczeństwa.*

Agent antywirusowy

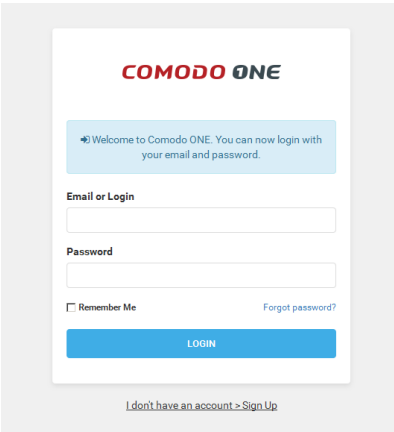
CES *(Comodo Endpoint Security) – program antywirusowy przeznaczony dla systemów Windows.*

1. Tworzenie nowego konta

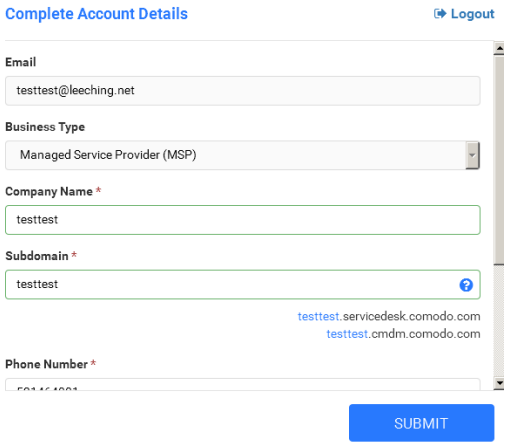
Zarządzanie oprogramowaniem COMODO IT & Security Manager nie wymaga od użytkownika posiadania własnego serwera. Konsola jest dostarczana i utrzymywana przez producenta w chmurze.

Aby uzyskać do niej dostęp:

1. W przeglądarce należy otworzyć adres https://dm.comodo.com oraz uzyskać dostęp TRIAL.
2. Na kolejnej stronie system poprosi o zalogowanie się jako istniejący użytkownik Comodo. Alternatywnie należy utworzyć nowe konto wypełniając wymagane pola. Konsola ITSM jest zintegrowana z konsolą Comodo One i tworząc dostęp do konsoli Comodo One zapewniamy sobie dostęp do COMODO IT & Security Manager. Należy wybrać konsolę Comodo One MSP.
3. Po otrzymaniu powiadomienia e-mail, należy kliknąć w link aktywacyjny, który przekieruje użytkownika na stronę podobną do poniższej (rysunek 1), gdzie należy zalogować się według wcześniej utworzonych danych z punktu 1.p2.
4. W następnym kroku podajemy nazwę naszej firmy i nazwę subdomeny – patrz rysunek 2.

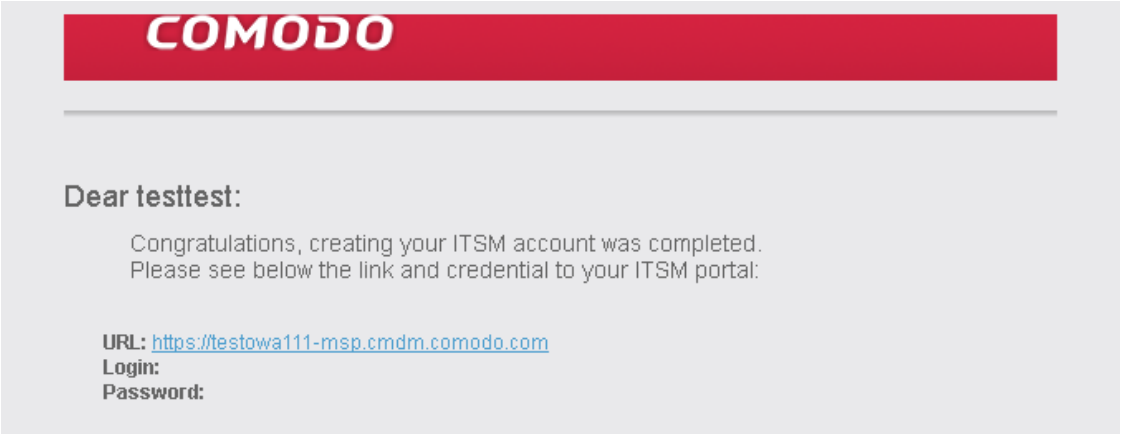


Rysunek 1 Konsola ITSM wymaga stworzenia konta COMODO ONE



Rysunek 2 Dane uzupełniające konto

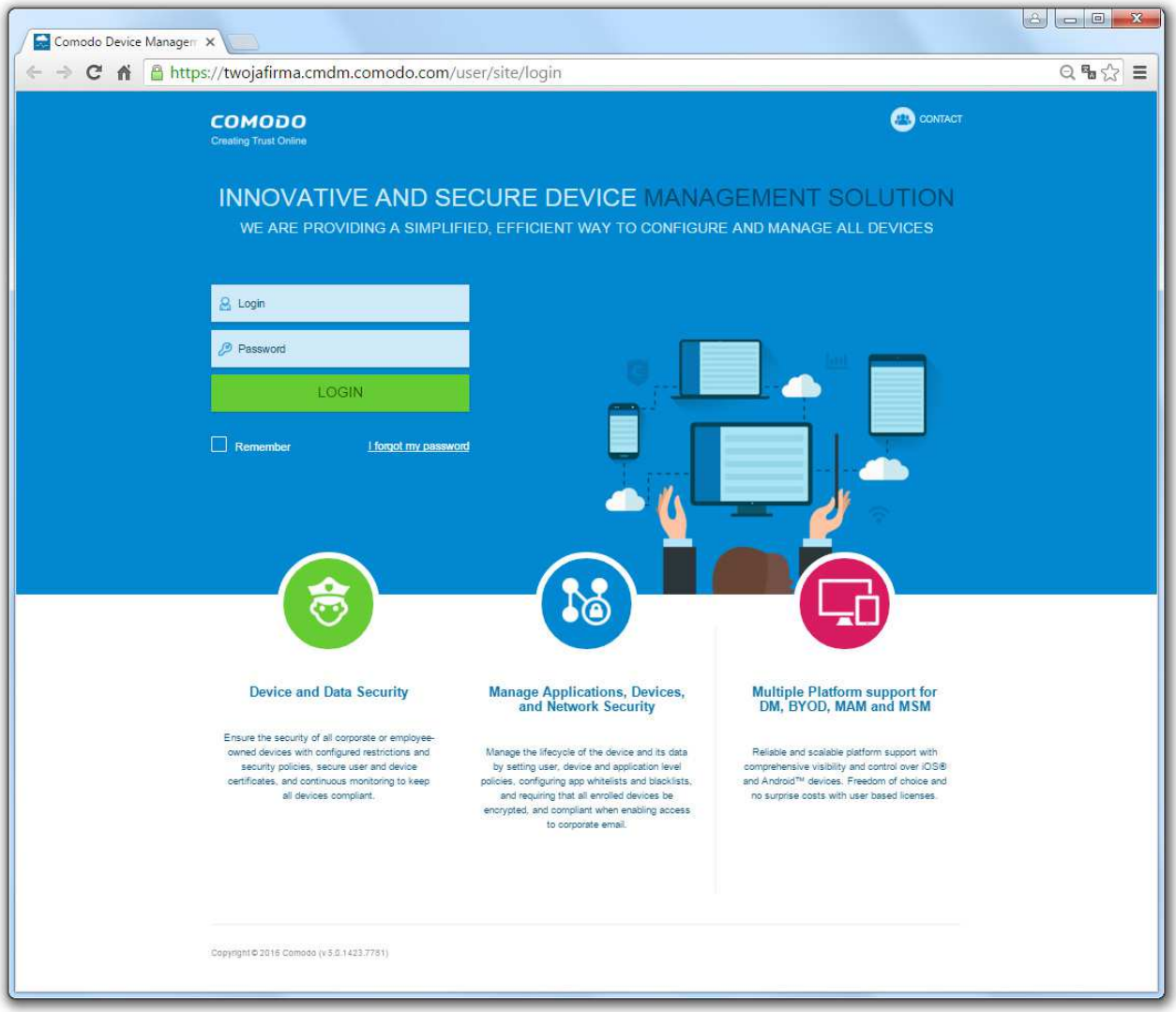
5. Comodo umożliwia zalogowanie się do konsoli wyłącznie poprzez unikatowy adres URL przypisany dla firmy (który podaliśmy w punkcie 4) oraz poprzez konto Comodo One gdzie z lewej strony zainstalowanych modułów wybieramy konsolę ITSM.



Rysunek 3 Wygenerowany e-mail z poświadczeniami

2. Logowanie do konsoli

Poniższy rysunek przedstawia stronę internetową konsoli, w której należy podać wcześniej wygenerowane poświadczenia. Jako loginu należy użyć *admin* oraz podać hasło, które zostało przysłane na adres e-mail administratora w procesie tworzenia dostępu do konsoli COMODO Device Manager (rysunek 4).



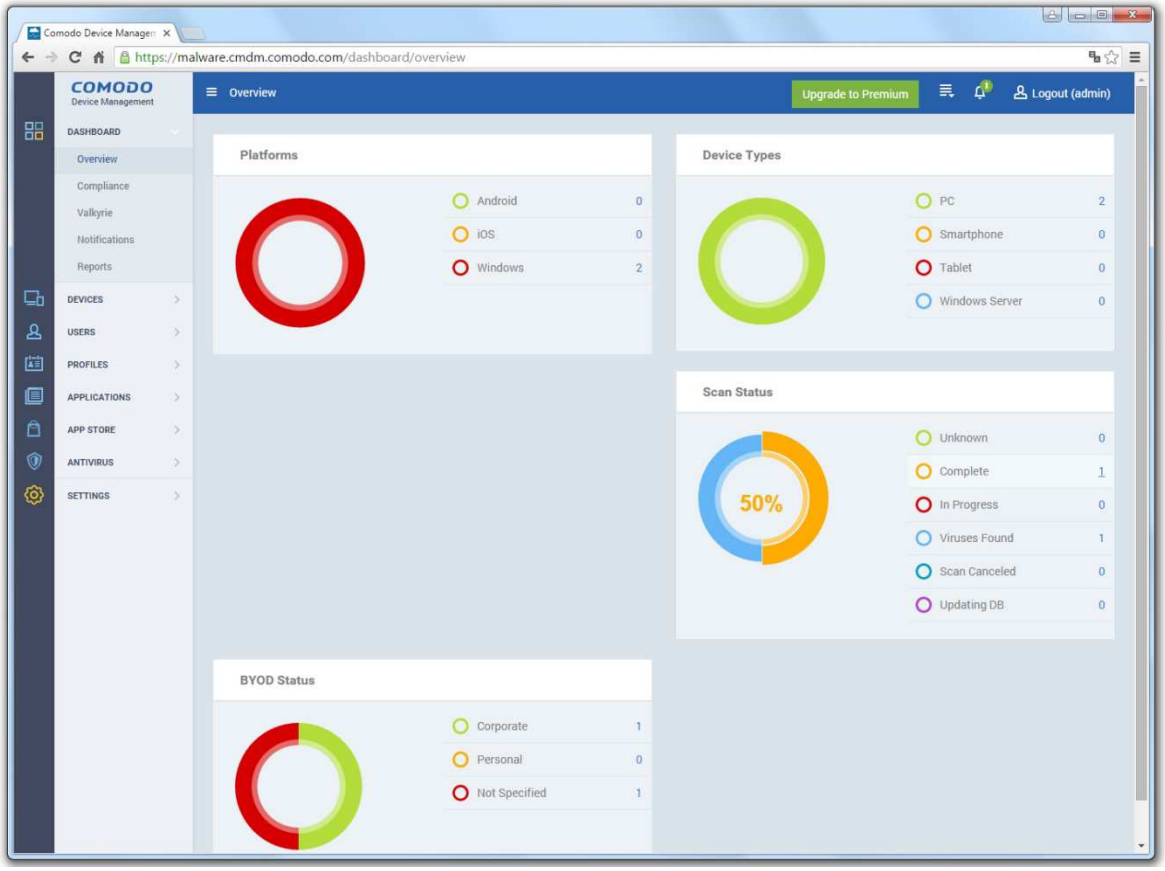
Rysunek 3 Strona internetowa konsoli COMODO IT & Security Manager

3. Konsola COMODO IT & Security Manager

Główne okno konsoli ITSM. Intuicyjny interfejs został podzielony na sekcje, które umożliwiają zarządzanie i monitorowanie punktami końcowymi. Z tego poziomu administrator może utworzyć konta nowych użytkowników, zarządzać już istniejącymi, skonfigurować profile bezpieczeństwa i powiązać urządzenia z profilami.

4. Dashboard

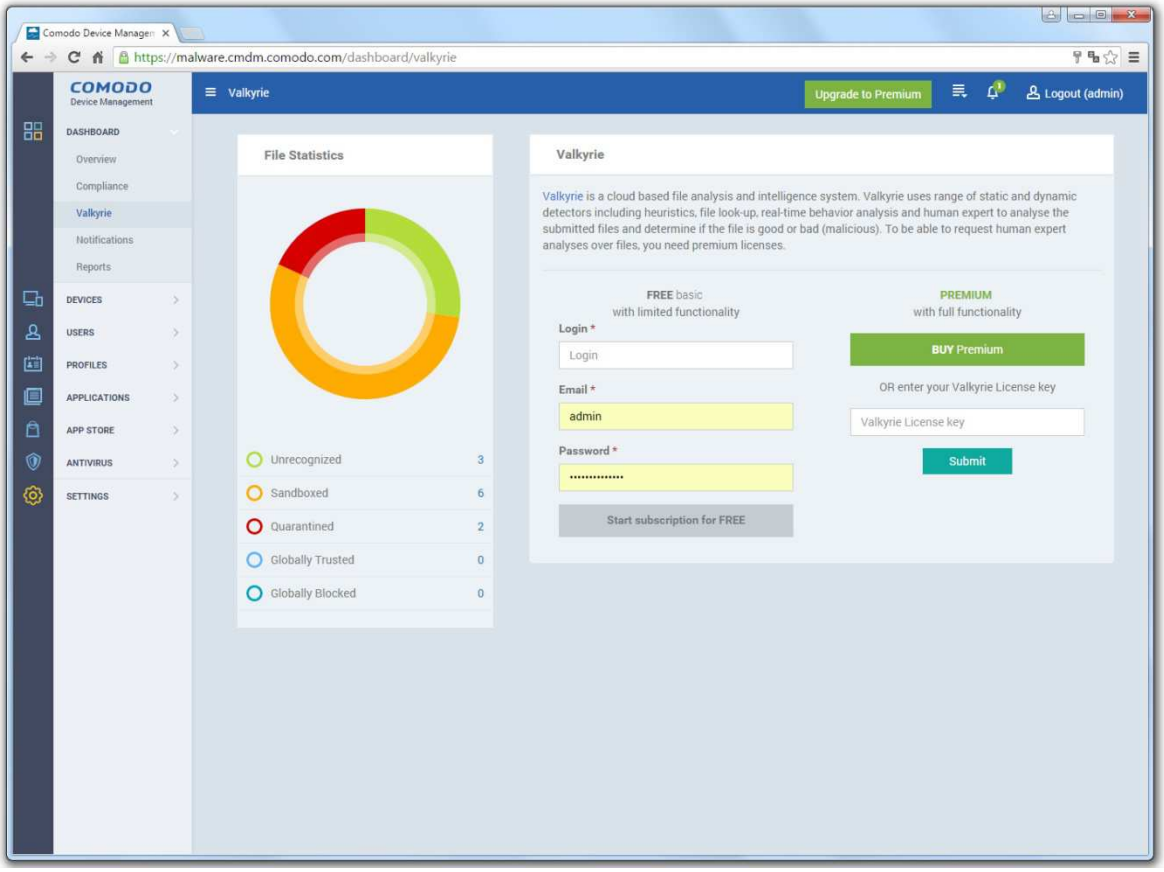
Poniższy rysunek przedstawia informacje z podziałem na systemy operacyjne, urządzenia i ich status.



5. Ocena zagrożeń Valkyrie

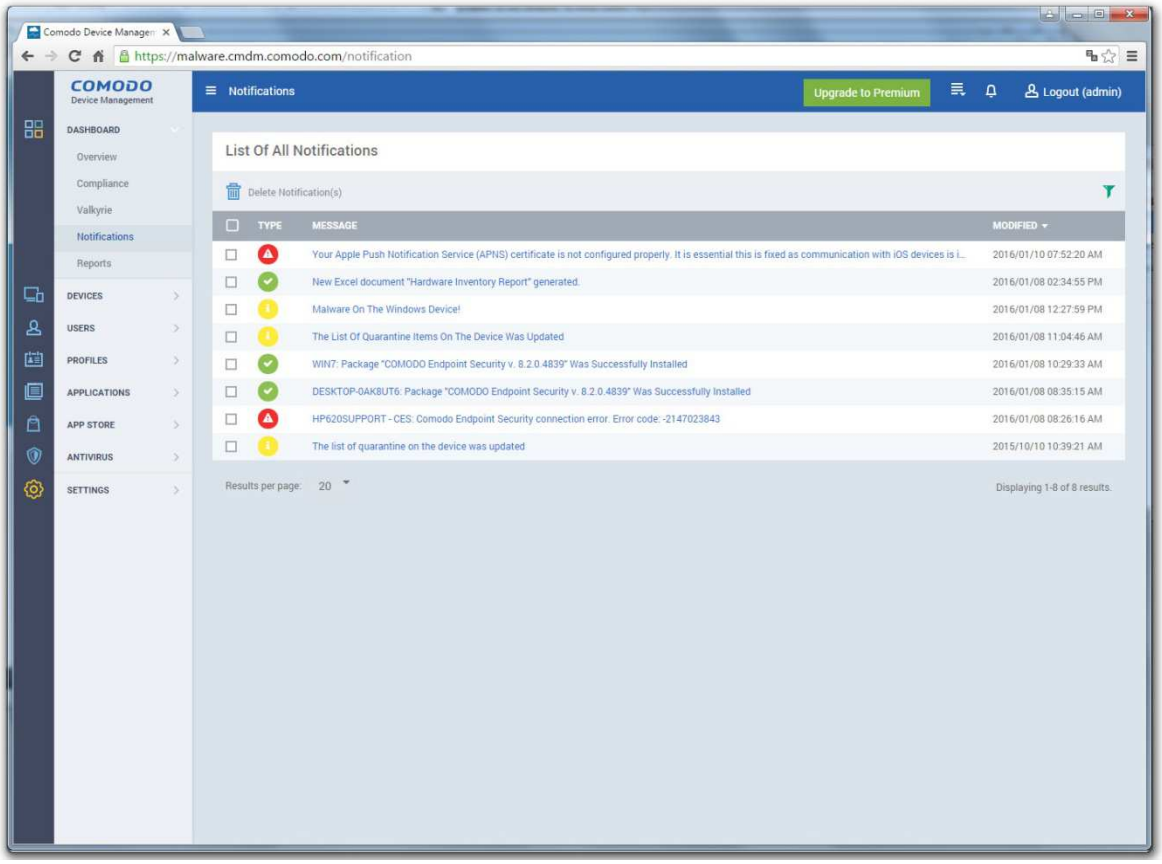
Konsola ITSM może zintegrować się z systemem COMODO Valkyrie, który do oceny bezpieczeństwa plików w czasie rzeczywistym wykorzystuje szereg czujników statycznych i dynamicznych oraz heurystykę i analizę behawioralną.

W tym oknie administrator ma wgląd w statystyki plików podejrzanych: nierozpoznanych i sklasyfikowanych jako bezpieczne przez agenta antywirusowego Comodo Endpoint Security, pliki uruchomione w piaskownicy, zagrożenia w kwarantannie oraz pliki zablokowane.



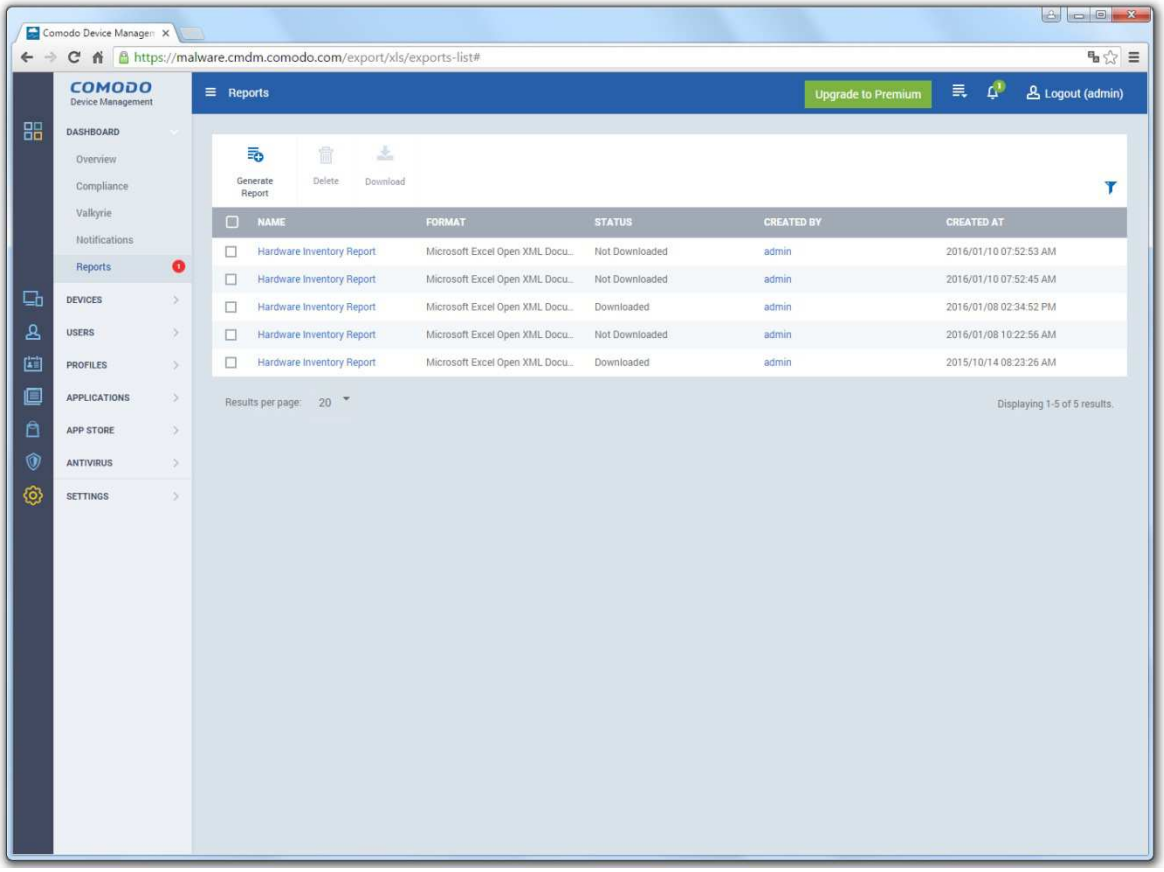
6. Powiadomienia o zdarzeniach

Lista wszystkich systemowych powiadomień, które wysyłane są z urządzenia po akcjach takich jak instalacja agenta, usunięcie aplikacji, wykryte zagrożenie, wygenerowany raport, itp.



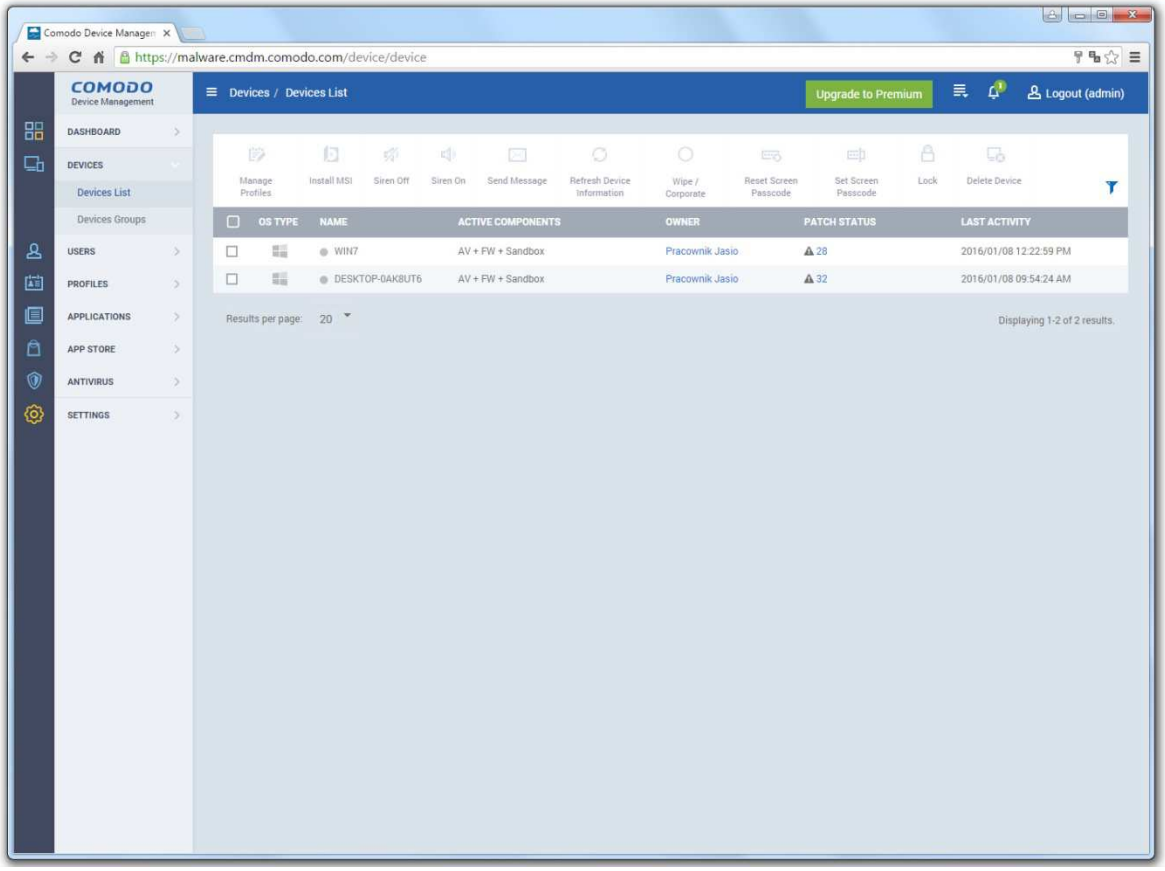
7. Generowanie raportów

Raporty pozwalają administratorom wyświetlać szczegółowe informacje o włączonych urządzeniach i szybko zidentyfikować oraz rozwiązać ewentualne problemy. Na przykład, na podstawie raportu, administrator może pobrać plik XML, XLSX i zobaczyć szczegółowe dane na temat konfiguracji sprzętowej urządzeń.



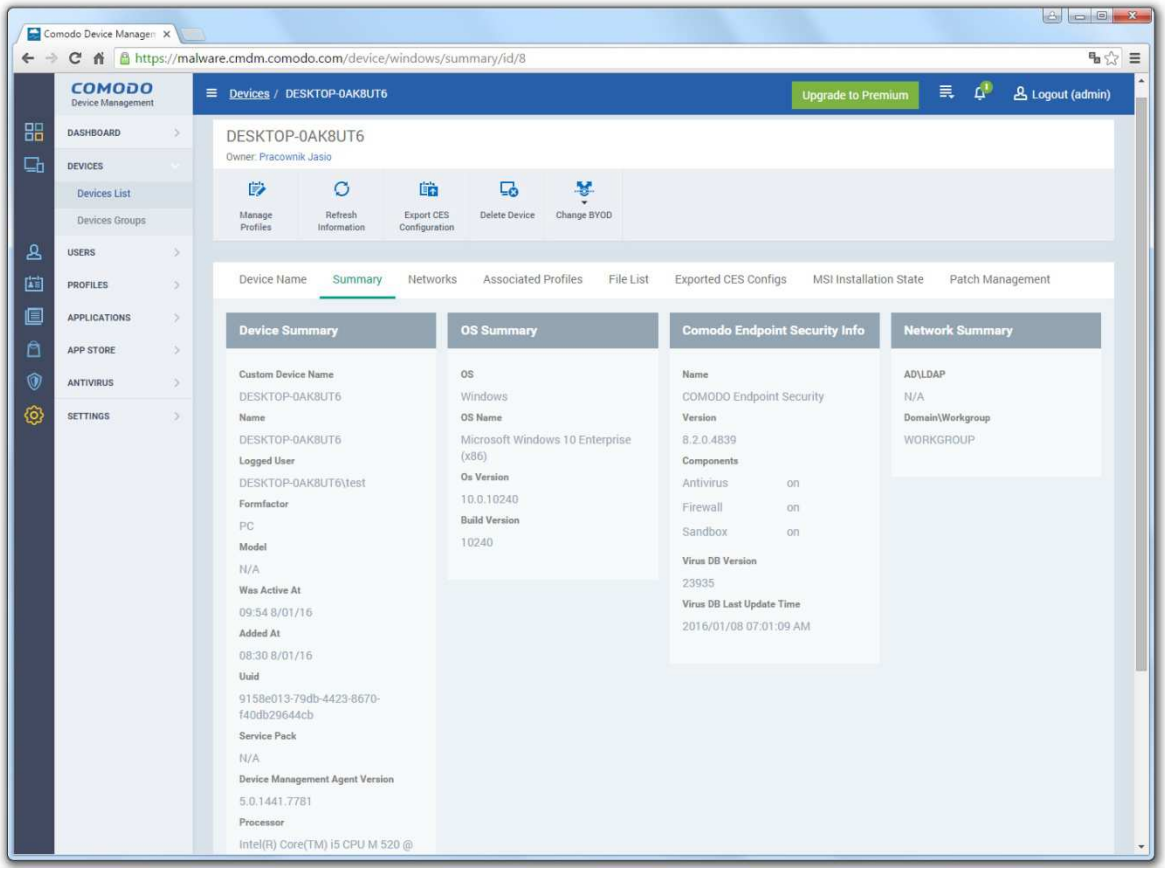
8. Urządzenia w konsoli

Zakładka DEVICES zawiera wszystkie informacje o urządzeniach mobilnych z systemem iOS, Android oraz stacjach roboczych z systemem Microsoft Windows, Windows Server, które mają dostęp do internetu za pośrednictwem medium przewodowego lub bezprzewodowego. Z tego poziomu możliwa jest zdalna instalacja agenta antywirusowego Comodo Endpoint Security na urządzeniach, na których zainstalowany jest tylko agent konsoli ITSM (*agent only* w kolumnie *active components*).



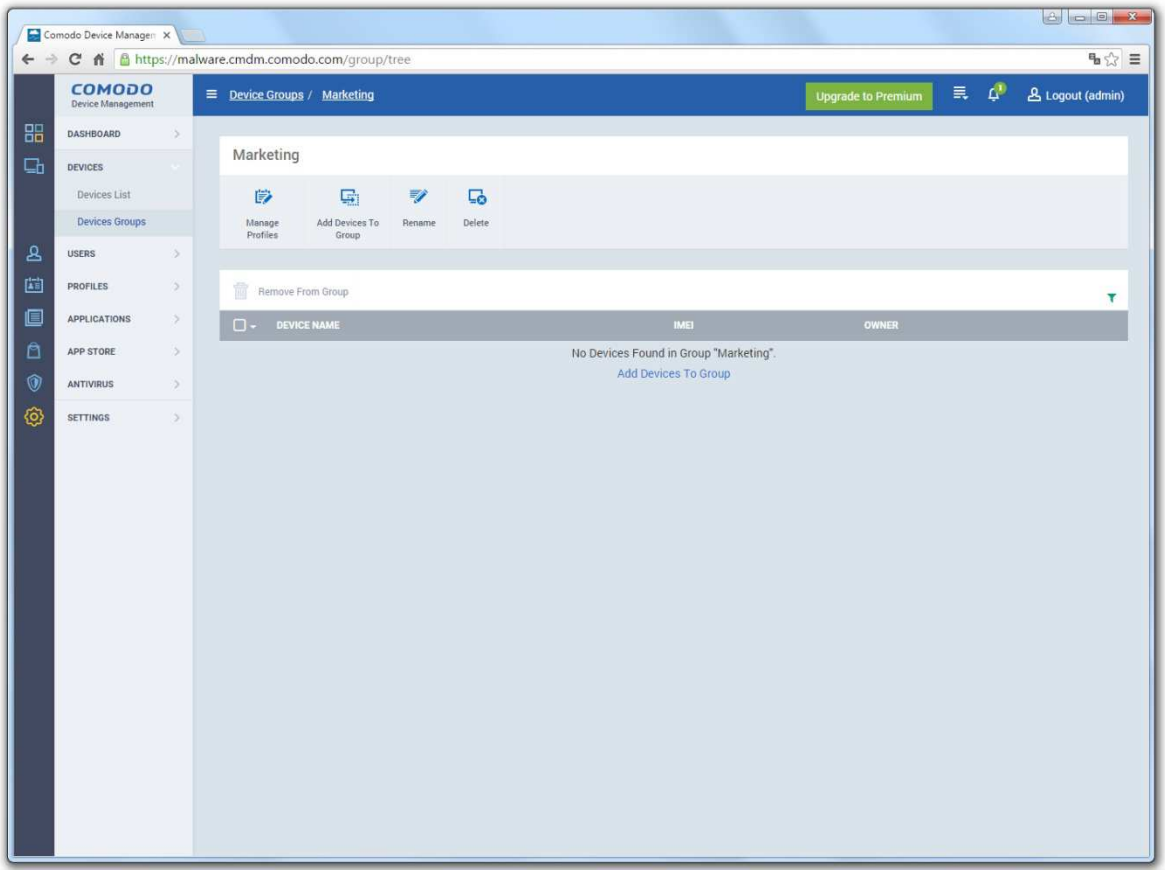
Administrator wybierając urządzenie z listy może wyświetlić o nim szczegółowe informacje, w tym nazwę komputera, która może być bezpośrednio z konsoli zmieniona, aby lepiej rozpoznać urządzenie; szczegółowe podsumowanie danych o systemie operacyjnym i konfiguracji sprzętowej, informacje o konfiguracji kart sieciowych; listy plików zaufanych, szkodliwych i nierozpoznanych przez agenta antywirusowego Comodo Endpoint Security.

W tym miejscu możliwe jest także odinstalowanie agenta antywirusowego z konkretnego urządzenia oraz pobranie i zainstalowanie łatek systemowych z Windows Update.



9. Podział na grupy urządzeń

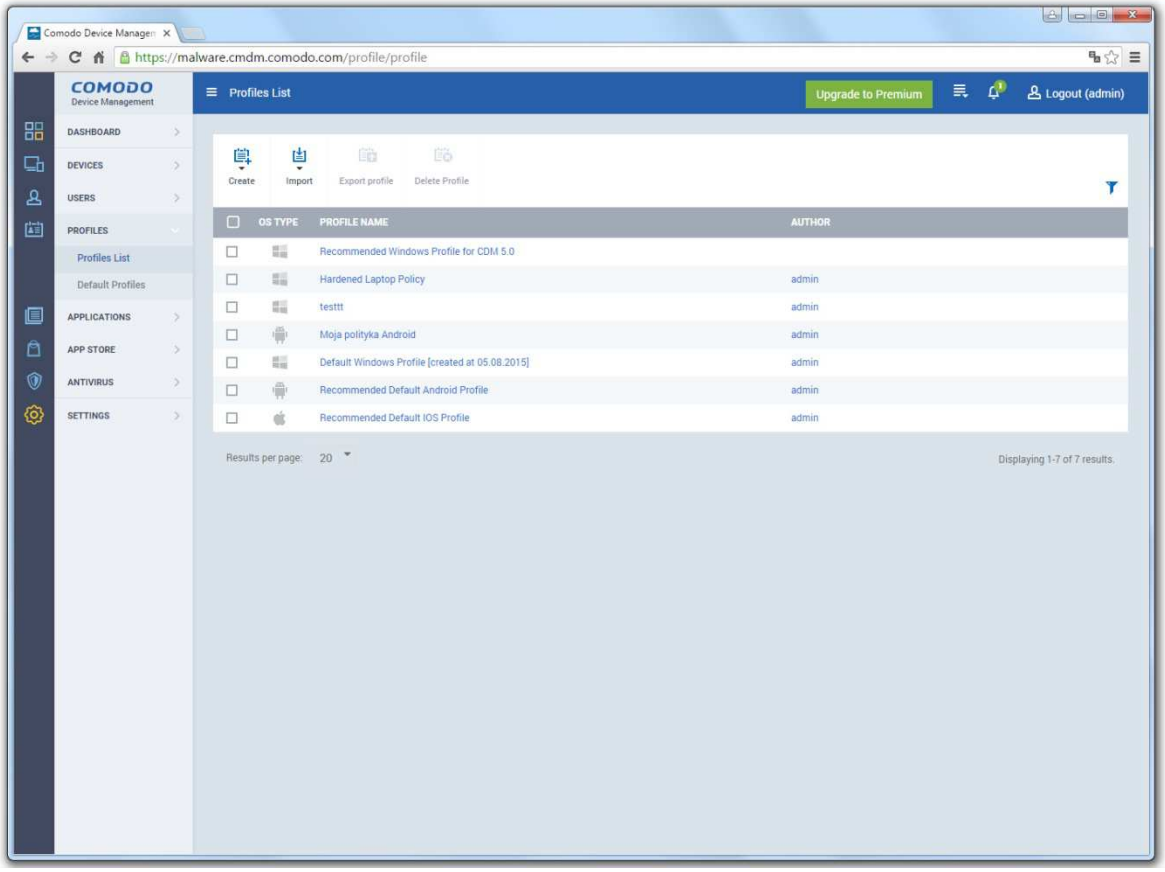
Grupy pozwalają odseparować urządzenia mobilne, takie jak smartfony i tablety od komputerów stacjonarnych. Dla danej grupy urządzeń, administrator kilkoma kliknięciami myszy jest w stanie przypisać profil bezpieczeństwa (politykę) rekomendowaną przed producenta lub stworzyć własną.



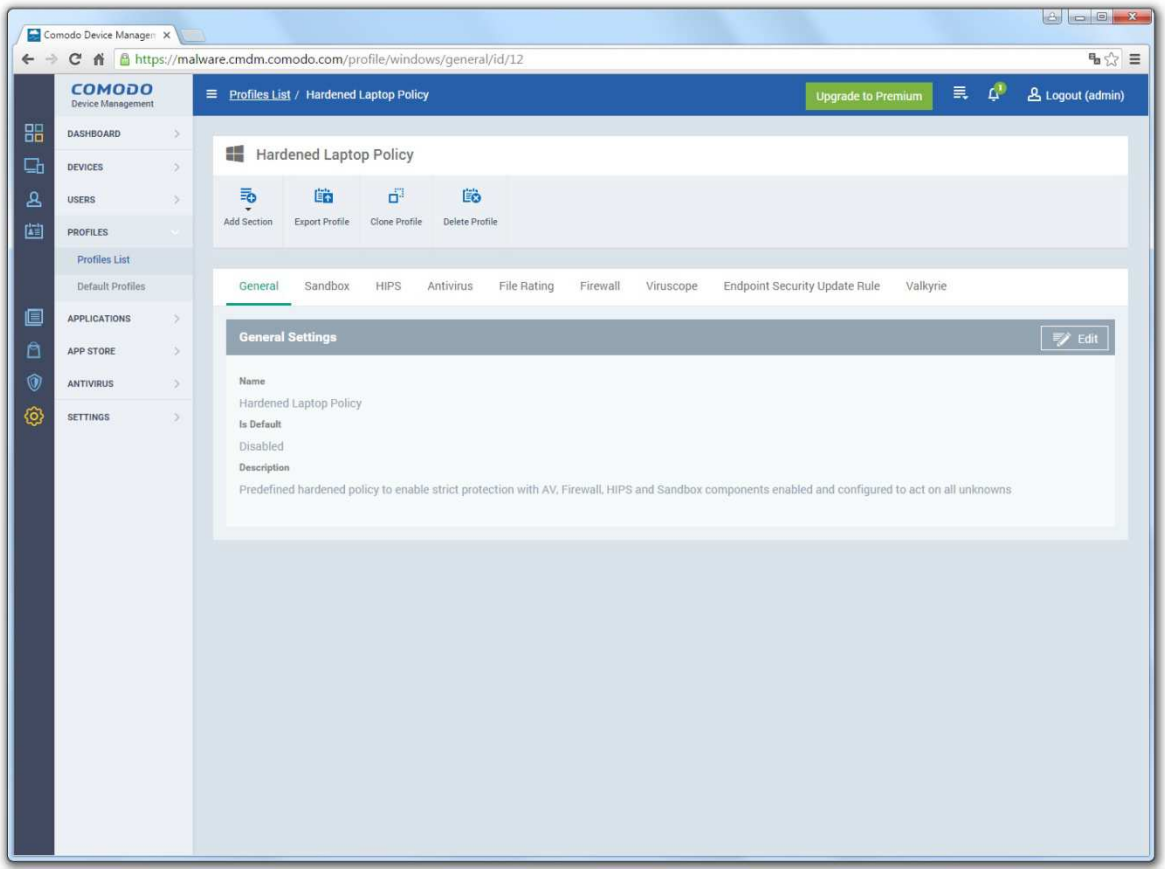
10. Profile bezpieczeństwa

Profile bezpieczeństwa są zbiorem ustawień stosowanym do przyporządkowania ustawień agentom Comodo, które określają prawa dostępu do sieci, ogólne zasady bezpieczeństwa, harmonogram skanowania antywirusowego i inne preferencje.

Profile zostały podzielone przez producenta na rekomendowane dla każdego rodzaju systemu operacyjnego, mogą być edytowane przed administratora i tworzone nowe, a także stosowane dla każdego urządzenia z osobna lub grupy urządzeń.



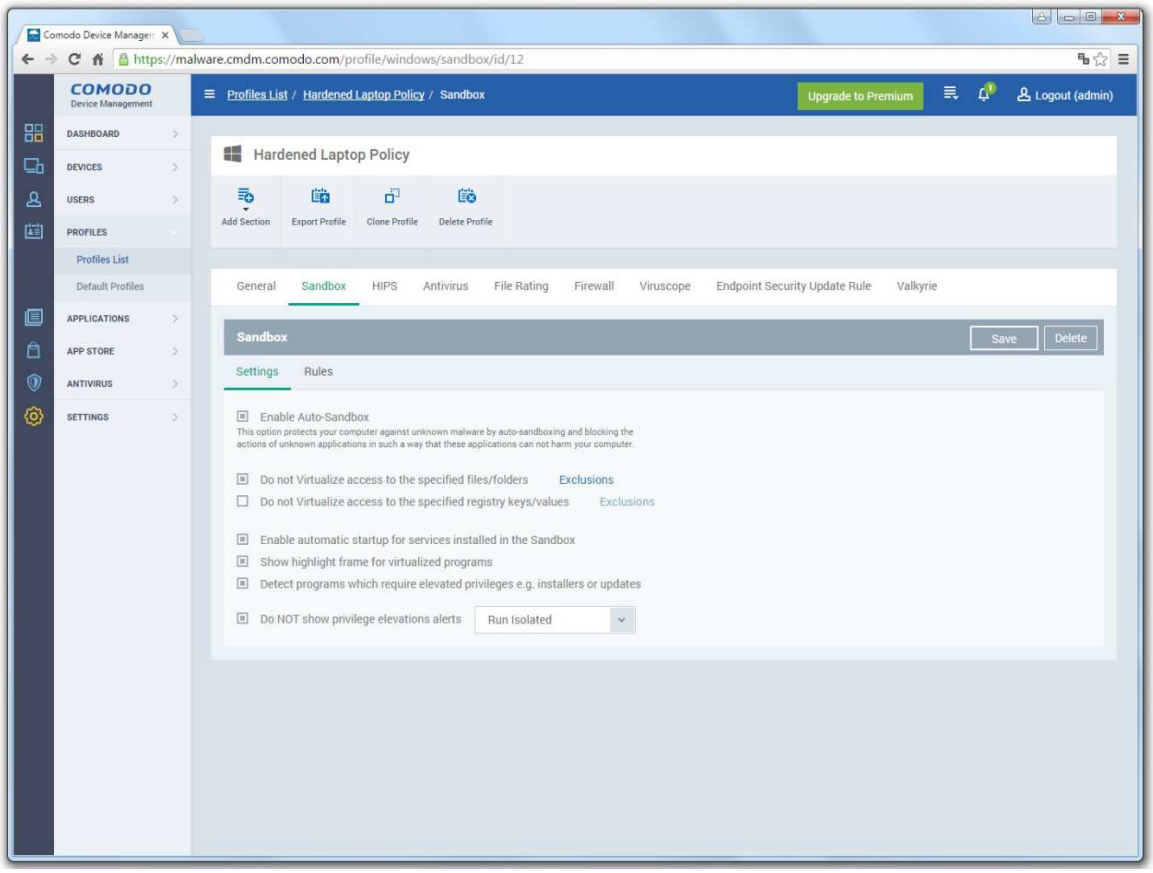
Ustawienia profili bezpieczeństwa dla agenta antywirusowego Comodo Endpoint Security podzielone są na funkcjonalności doskonale rozpoznawalne przez użytkowników aplikacji Comodo. Administrator uzyskuje odwzorowane ustawienia 1:1, identyczne z tymi, które znajdują się w Comodo Internet Security lub Comodo Endpoint Security.



11. Profile Automatyczna piaskownica

Konfigurowanie modułu automatycznej piaskownicy, która uruchamia w bezpiecznym kontenerze nieznane aplikacje. Ustawienia zaawansowane umożliwiają przeglądanie, zarządzanie, dodawanie aplikacji, które zawsze powinny być uruchamiane wewnątrz kontenera. Dzięki temu, potencjalnie szkodliwy program nie będzie miał możliwości uszkodzenia komputera, zainfekowania go, ponieważ będzie odizolowany od systemu operacyjnego oraz plików.

Pozwoli to bezpiecznie uruchamiać aplikacje, które nie są w 100% bezpieczne.

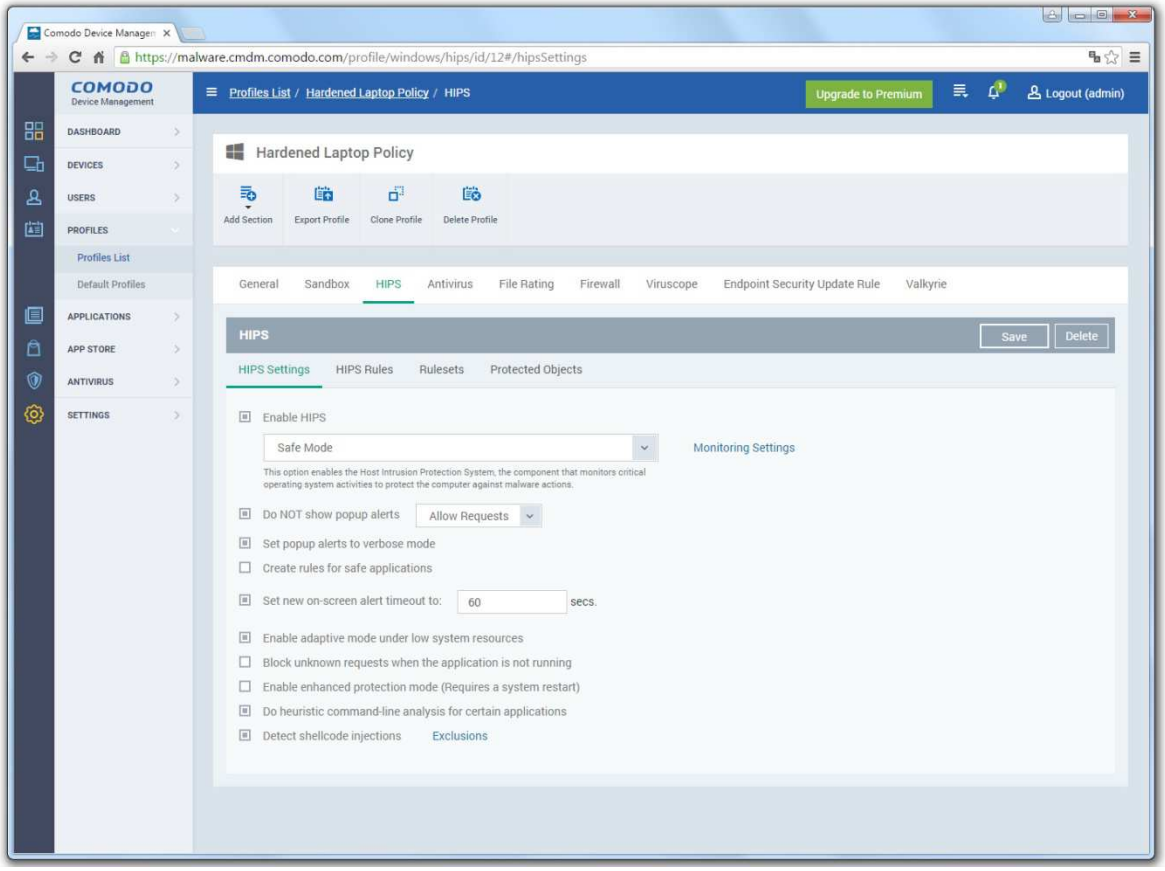


12. Profile HIPS

Moduł HIPS chroni pliki systemowe, krytyczne foldery i klucze rejestru - zapobiega ich nieautoryzowanym modyfikacjom przez złośliwe programy. Stale monitoruje aktywność systemu i pozwala uruchomić pliki wykonywalne i procesy, jeżeli są one zgodne z obowiązującymi ustawieniami bezpieczeństwa. Dla przeciętnego użytkownika, Comodo już na ustawieniach domyślnych zapewnia bardzo wysokim poziom ochrony bez żadnej ingerencji w ustawienia.

Uwaga dla początkujących: HIPS monitorując pliki wykonywalne, a więc każdy program, aplikację, np. po uruchomieniu programu Microsoft Word, plik wykonywalny to "winword.exe", który inicjuje komputer do uruchomienia aplikacji Word. Inne typy plików wykonywalnych obejmują rozszerzenia .dll .cpl .drv, inf, OCX, SCR, .pf, sys.

Nie wszystkie pliki wykonywalne są bezpieczne. Niektóre z nich są niezwykle często wykorzystywane jako medium do przenoszenia złośliwego kodu z komputera na komputer i mogą usuwać cenne dane, wykradać loginy i hasła, uszkodzić system i wiele więcej.

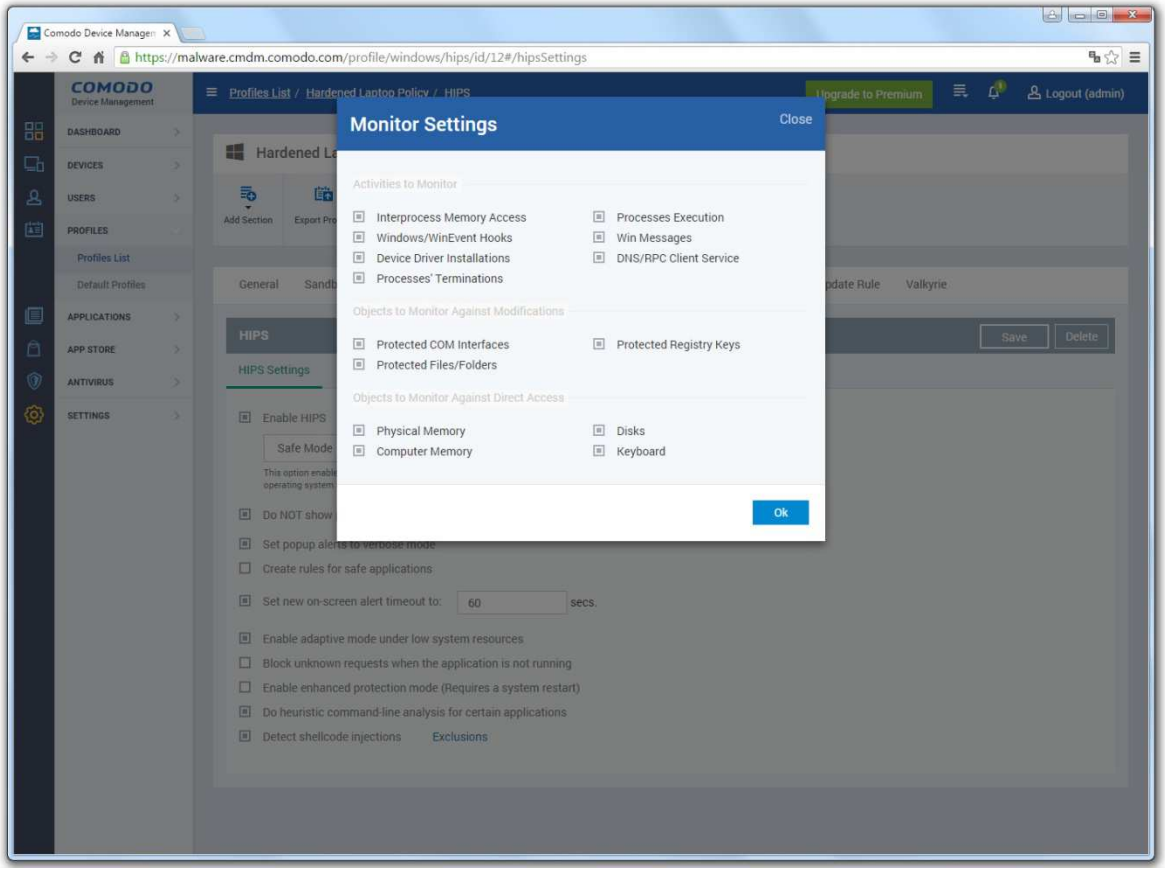


Już na ustawieniach domyślnych HIPS wykorzystuje kilkanaście procedur do ochrony systemu przed szkodliwym oprogramowaniem.

Comodo przed przechwytywaniem informacji z procesów systemowych wykorzystuje autorskie mechanizmy ochrony, które mogą zmodyfikować dane w pamięci operacyjnej i wstrzyknąć szkodliwy kod, zapisywać uderzenia w klawiaturę, kraść poufne dane poprzez wysłanie informacji z jednego procesu do drugiego.

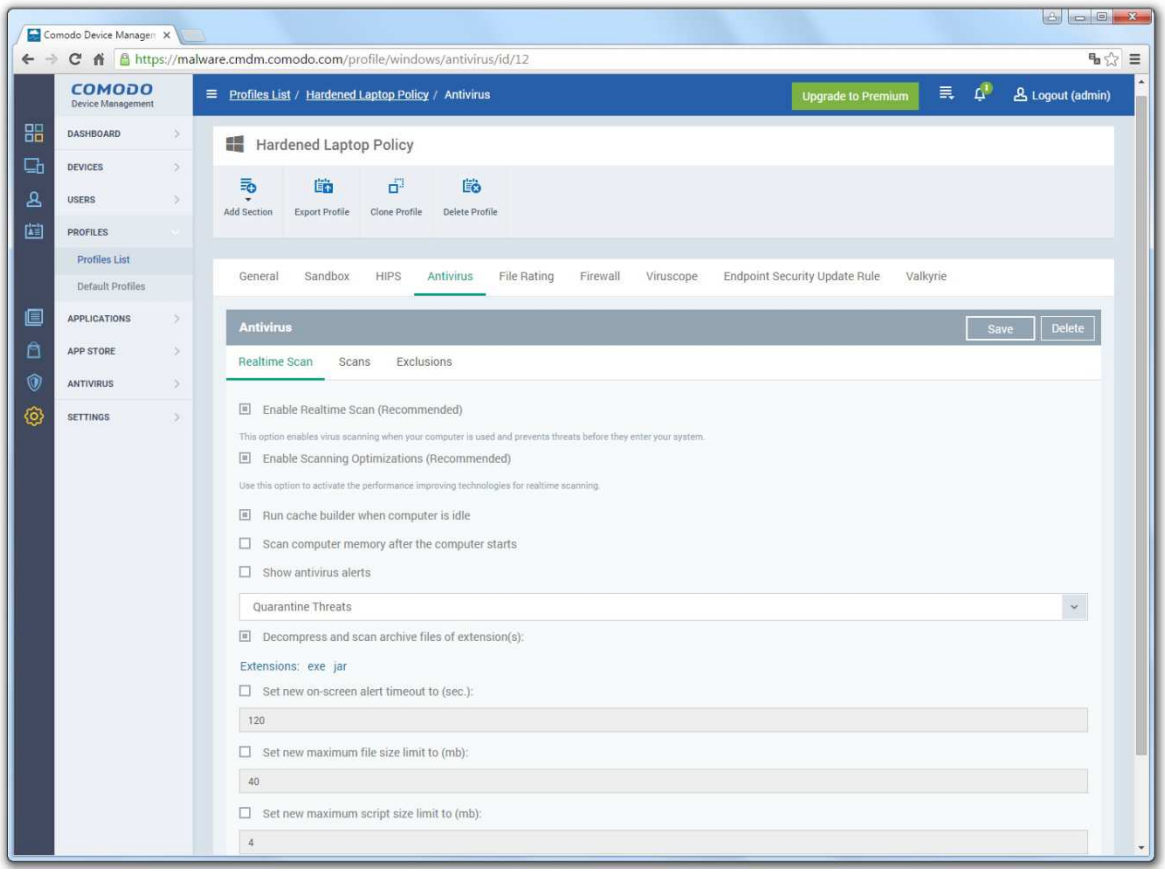
HIPS chroni też aplikacje i procesy przed hakami na API systemu Windows. Wykorzystanie tych funkcji w kodzie wirusa może pozwolić przechwytywać wiadomości, akcje podjęte myszą, wciskane klawisze, zanim trafią do docelowej aplikacji. Chronione są także sterowniki systemowe dysków, karty graficznej, kart sieciowych, urządzeń USB, monitorów, odtwarzaczy DVD, itp.

Ustawienia te zabezpieczają procesy Comodo przed ich nieautoryzowanym zakończeniem ze strony Trojanów, wirusów oraz chronią system operacyjny przed modyfikacją serwerów DNS.



13. Profile Antywirus

Ustawienia antywirusa pozwalają m.in. na zdefiniowanie harmonogramu skanowania, dodanie plików i katalogów do wykluczenia ze skanowania, ustawienia silnika antywirusowego, który chroni system w czasie rzeczywistym, skanowanie pamięci operacyjnej przy starcie systemu, dodanie konkretnych rozszerzeń plików do skanowania, wykluczenie plików ze skanowania większych niż zdefiniowana waga (w MB), ustawienie heurystyki skanowania.



14. Profile ocena reputacji

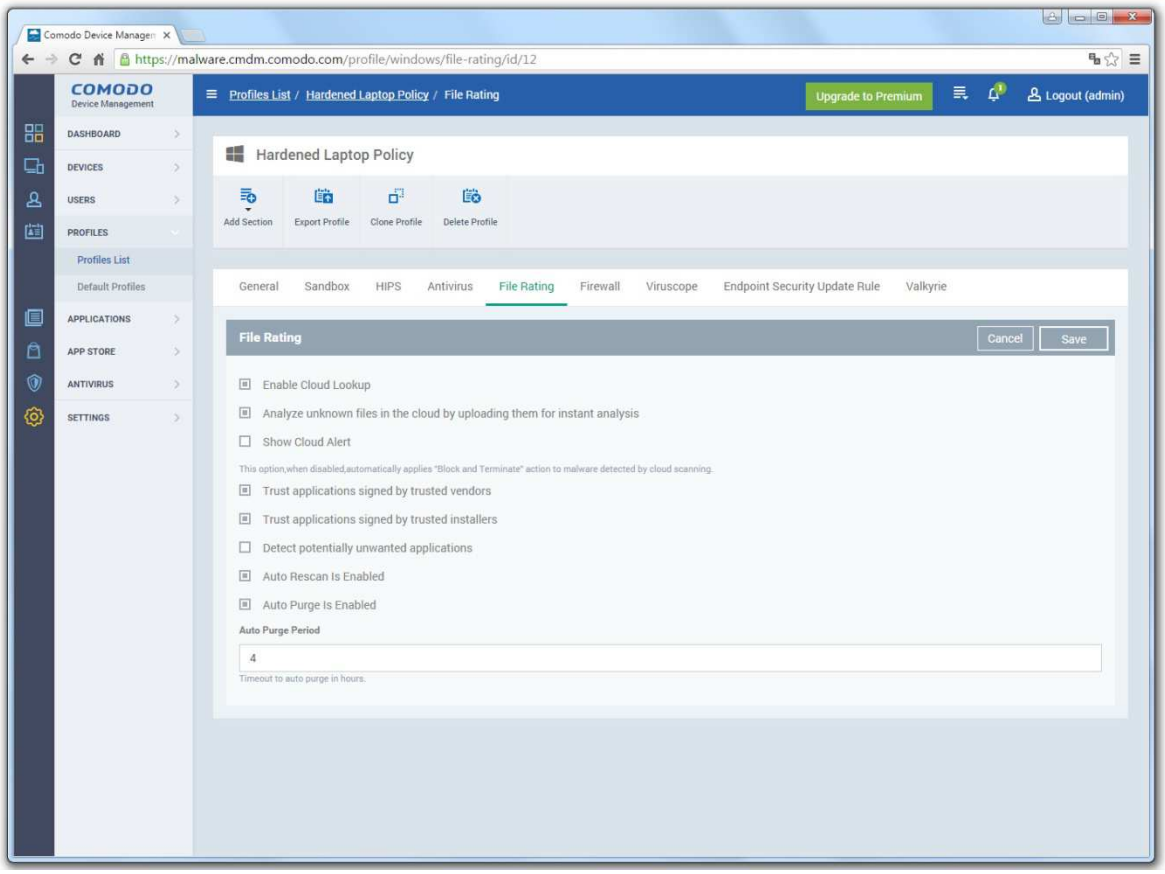
Ocena reputacji plików w chmurze (File Rating Files) sprawdza, które pliki w systemie są bezpieczne i porównuje je z bazą plików w chmurze Comodo. Za pierwszym razem, kiedy użytkownik lub inna aplikacja zażąda dostępu do określonego pliku, będzie mu przyznany status zgodnie z zasadami:

Bezpieczny – jeśli plik znajduje się na liście zaufanych plików, jeśli aplikacja jest na liście zaufanych dostawców oprogramowania i jeśli aplikacja znajduje się na stale aktualizowanej bezpiecznej liście plików Comodo.

Zaufane pliki są wykluczone z monitorowania przez HIPS. Pozwala to zmniejszyć zużycie zasobów sprzętowych (procesor, pamięć RAM).

Z drugiej strony, pliki, które zostały zidentyfikowane jako szkodliwe, zostaną dodane do listy zablokowanych plików i nie uzyskają dostępu do innych procesów i kont użytkowników.

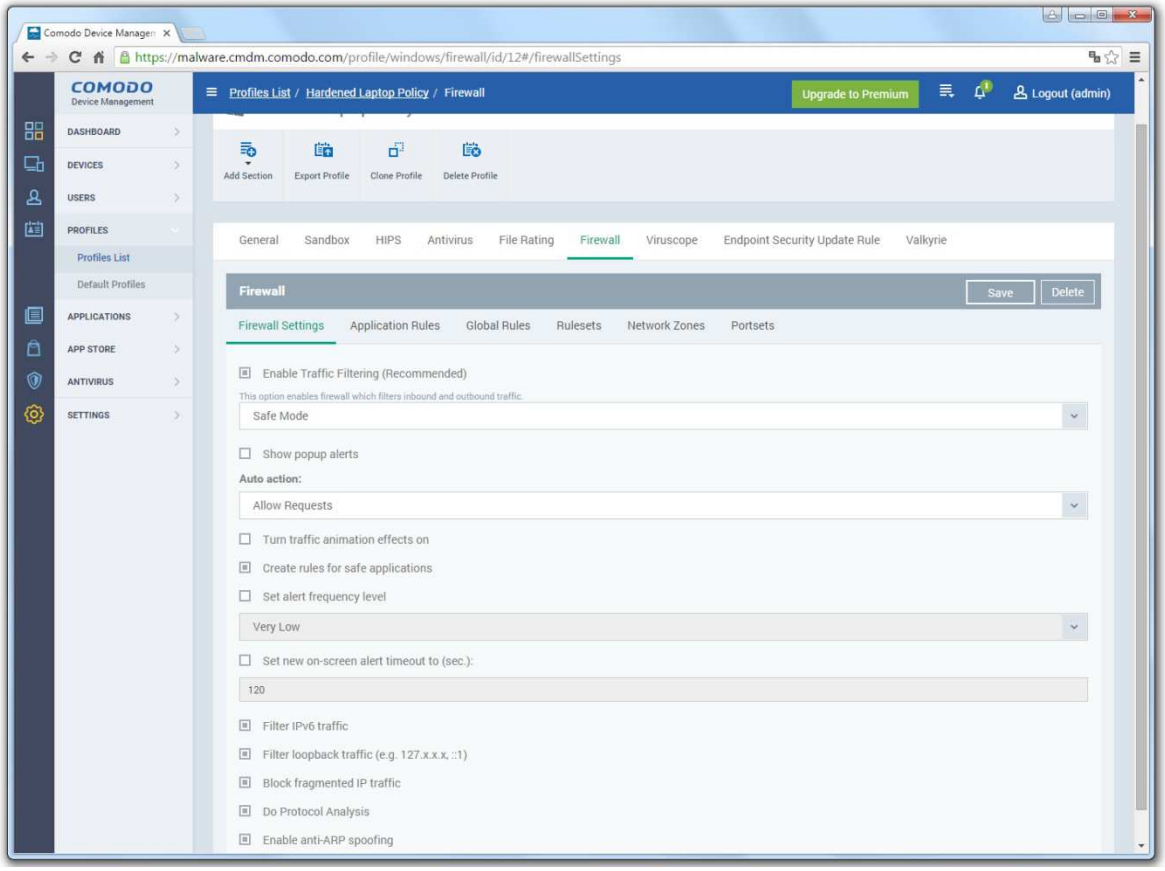
Pliki, które nie mogą być rozpoznawane przez system oceny plików Comodo, są dodawane do listy "Nierozpoznane" (Unrecognized), skąd mogą zostać usunięte, przesłane do analizy lub oznaczone jako bezpieczne.



15. Profile Firewall

Składnik Firewall skanuje ruch przychodzący i wychodzący. Sprawdza, czy cały ruch sieciowy *z i do* komputera jest zgodny z zasadami, potrafi ukryć porty stacji roboczej minimalizując ryzyko ataku i blokuje złośliwe oprogramowanie, które próbuje przesłać wykradzione dane do serwerów cyberprzestępców.

Comodo Firewall umożliwia m.in. zdefiniowanie reguł dla aplikacji, które mogą łączyć się z internetem, filtrować ruch IPv4 i IPv6 i chroni przed atakami ARP-spoofing, ARP- poisoning. Administrator może definiować ruch dla protokołów IP, ICMP, TPC, UDP, HTTP, POP3, SMTP i ich portów oraz wiele więcej.

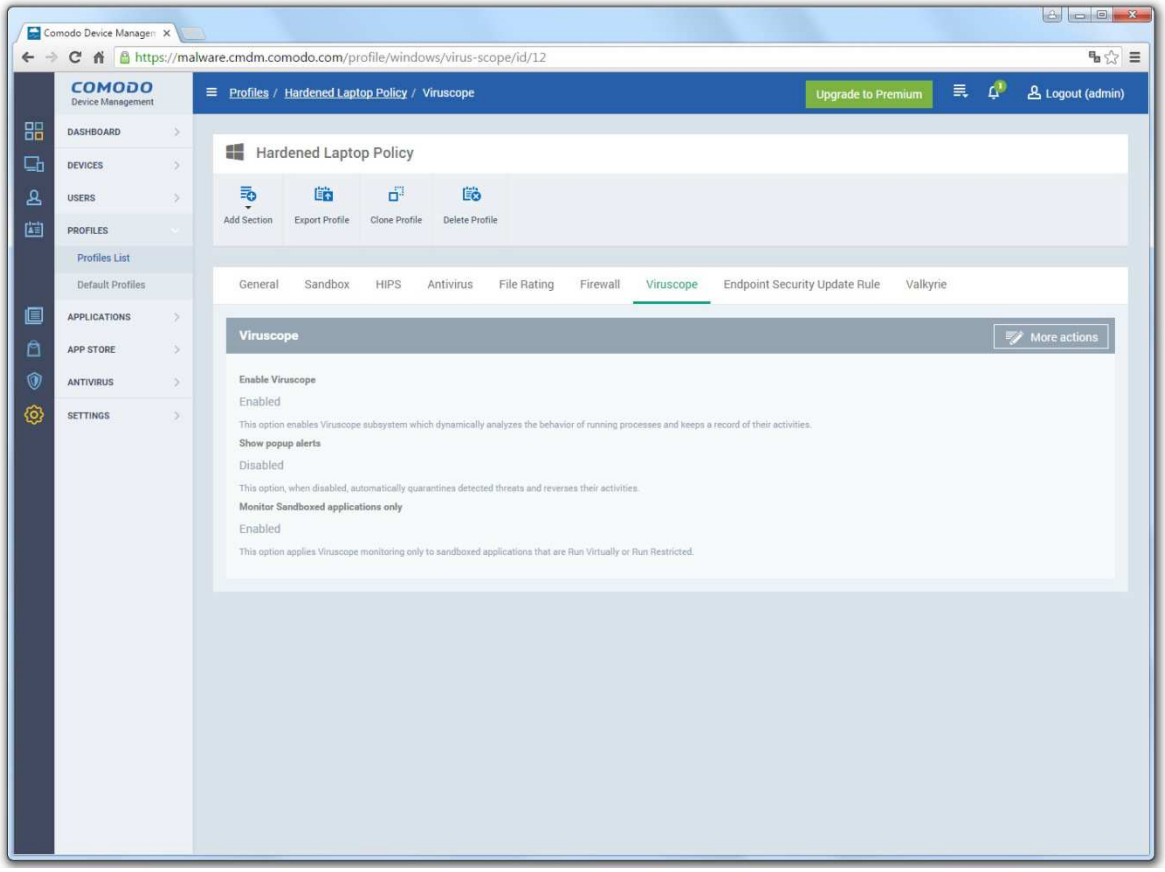


16. Profile Viruscope

Viruscope tworzy kolejną warstwę wykrywania szkodliwego oprogramowania i stanowi cenny dodatek do podstawowego procesu monitorowania funkcjonalności w Defense+.

Viruscope monitoruje działania procesów uruchomionych na komputerze i informuje użytkownika alertem, jeśli aplikacje mogą potencjalnie zagrażać prywatności i bezpieczeństwu.

Viruscope wykrywa złośliwe oprogramowania zero-day poprzez analizę zachowania i działania aplikacji. Jeśli wykryte zachowanie odpowiada znanemu wzorcowi malware, Viruscope wygeneruje alarm, który pozwoli przenieść wirusa do kwarantanny i odwrócić wprowadzone szkodliwe zmiany.

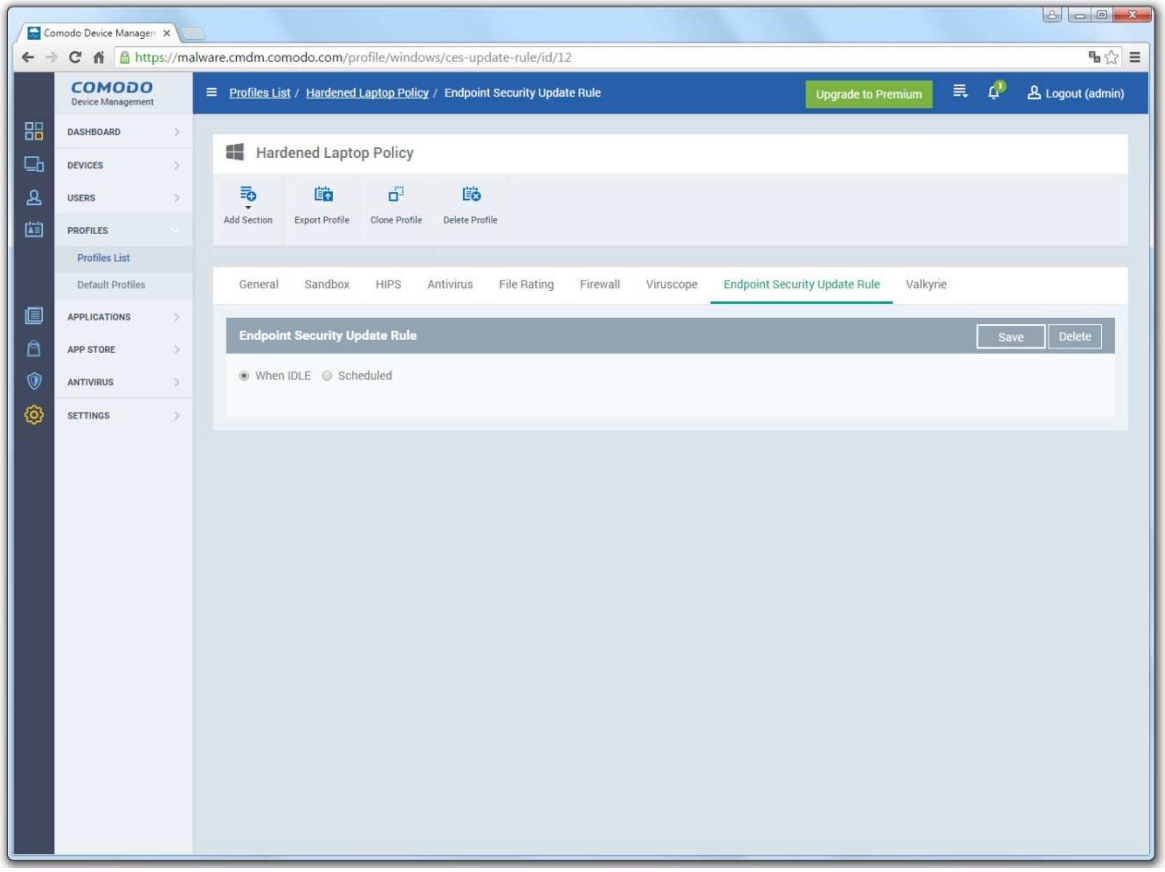


17. Automatyczna aktualizacja

Zakładka ta odpowiada za automatyczną aktualizację agenta antywirusowego Comodo Endpoint Security według zdefiniowanych reguł – podczas bezczynności systemu operacyjnego lub według zdefiniowanego harmonogramu.

Bazy danych sygnatur wirusów aktualizowane są automatycznie. Manualna aktualizacja sygnatur dostępna jest w sekcji:

ANTIVIRUS ->DEVICES – UPDATE ANTIVIRUS DB

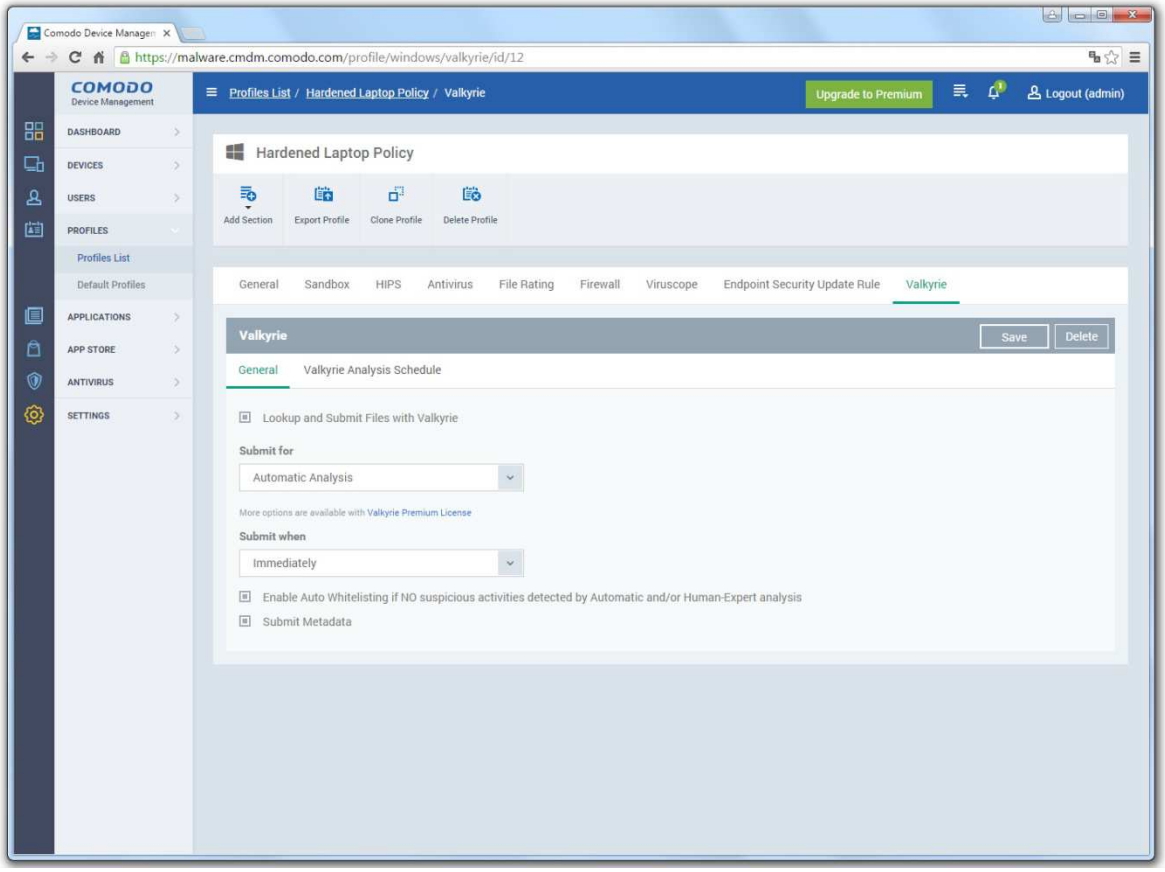


18. Profile Valkyrie

Valkyrie to oparty na chmurze system analizy pików, który całkowicie różni się od konwencjonalnej techniki wykrywania szkodliwego oprogramowania na podstawie sygnatur. Technologia ta obejmuje statyczną oraz dynamiczną analizę przesłanych plików.

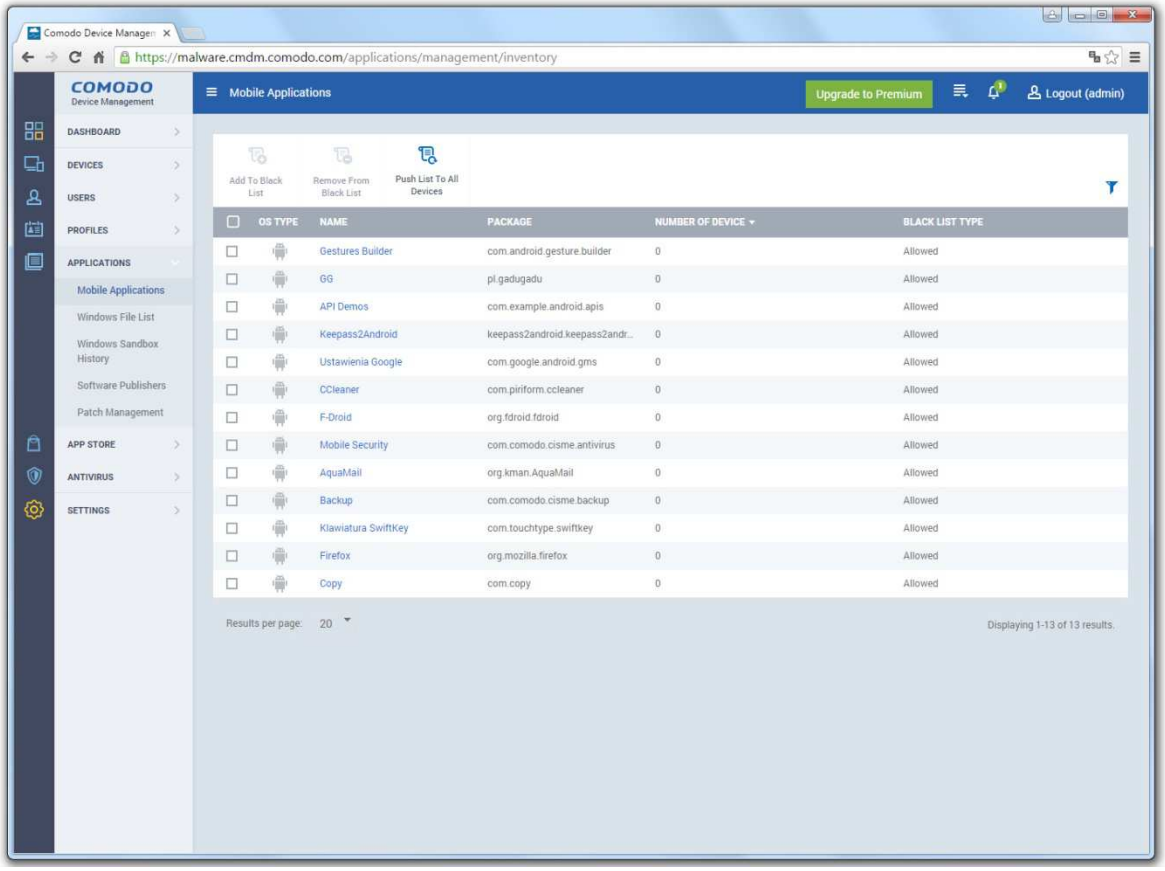
Administrator może zdecydować, *kiedy i czy* wysyłać metadane nierozpoznanych plików do analizy. Więcej opcji dostępnych jest po wykupieniu konta *premium* dla tej funkcjonalności.

Nieznane pliki, które nie będą wykazywać żadnej szkodliwości w przypadku analizy przez system Valkyrie oraz ekspertów z firmy Comodo, będą automatyczne oznaczone jako zaufane.



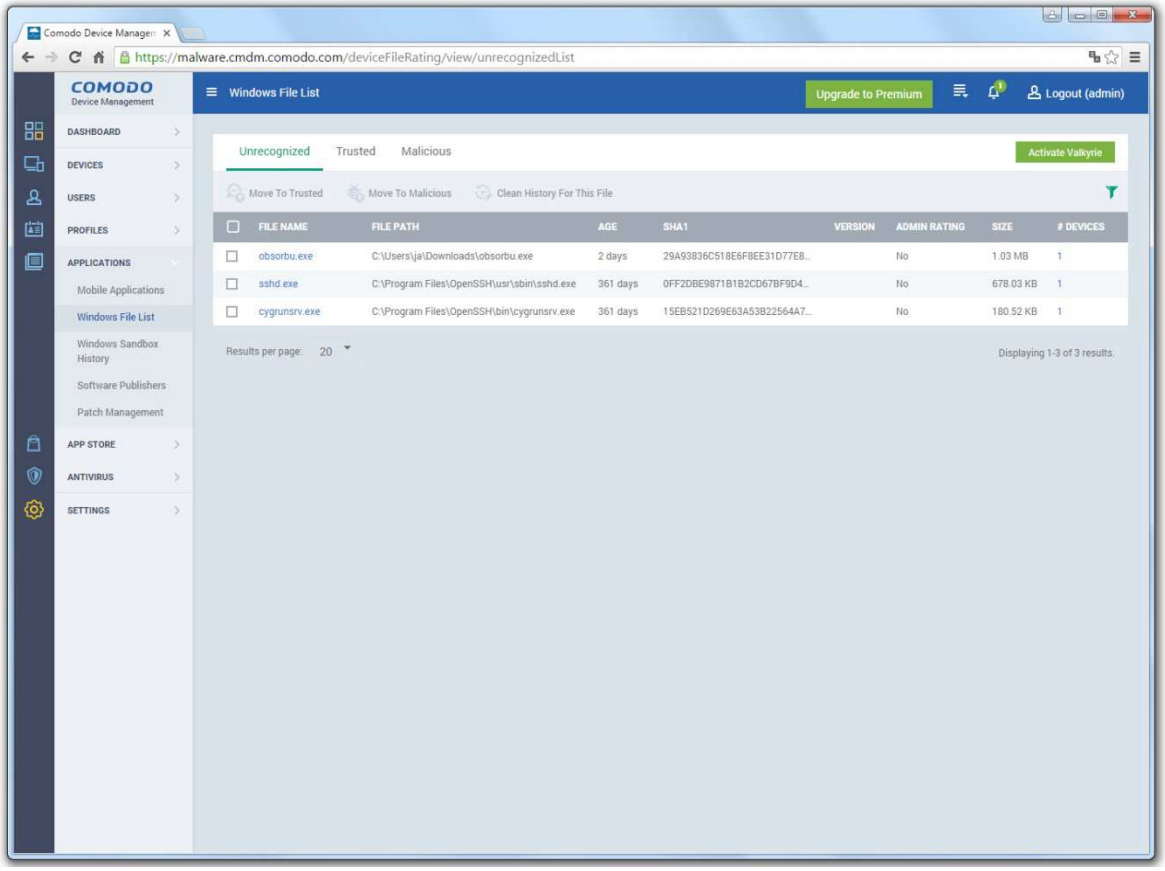
19. Kontrola aplikacji

COMODO IT & Security Manager umożliwia administratorom na wgląd w zainstalowane aplikacje na urządzeniach mobilnych, ich usuwanie oraz dodawanie do czarnych list programów, które nie powinny być uruchamiane w pracy.



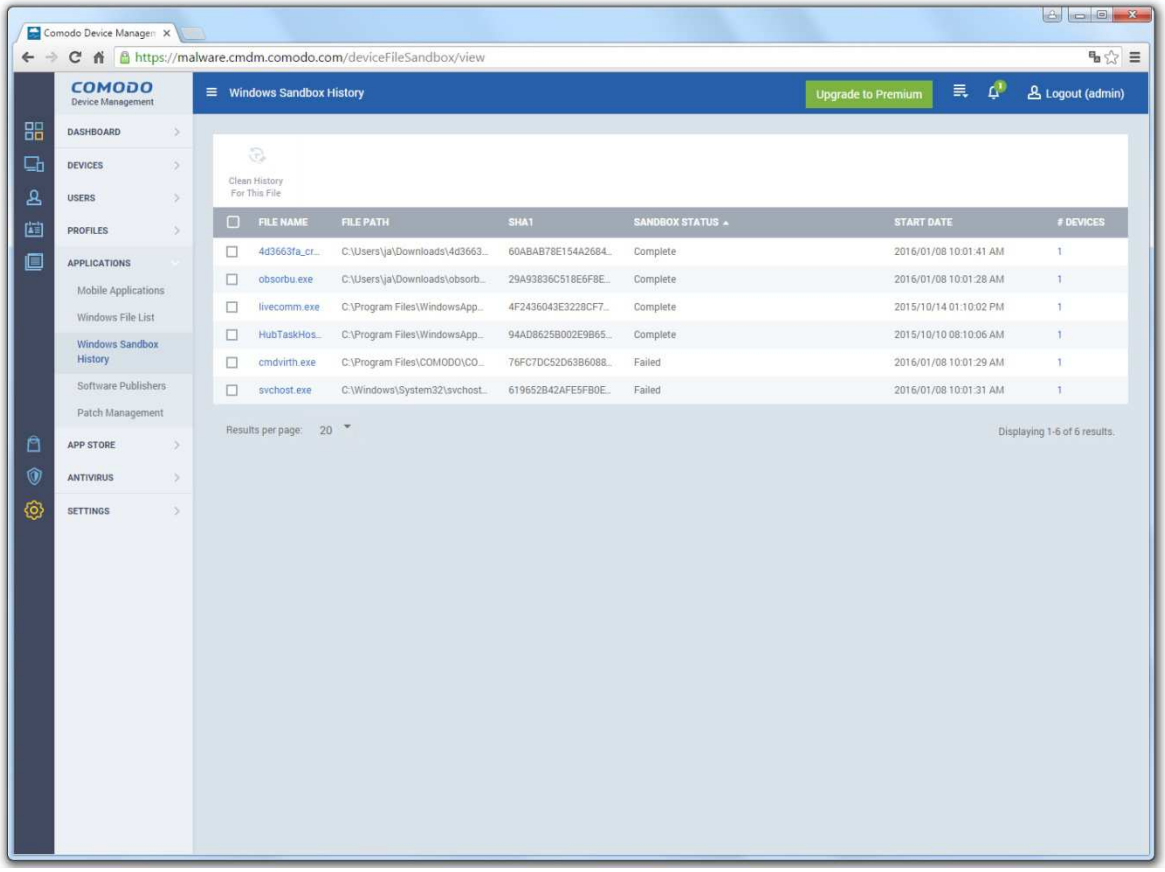
20. Kategoryzowanie plików

Po zainstalowaniu agentów antywirusowych Comodo Endpoint Security na stacjach roboczych z system Windows, administrator może przejrzeć pliki, które są przez Comodo nierozpoznane, i które na podstawie zdefiniowanego harmonogramu w systemie Valkyrie zostaną przesłane do analizy. Z tego poziomu, pliki te mogą zostać dodane do listy plików bezpiecznych lub szkodliwych.



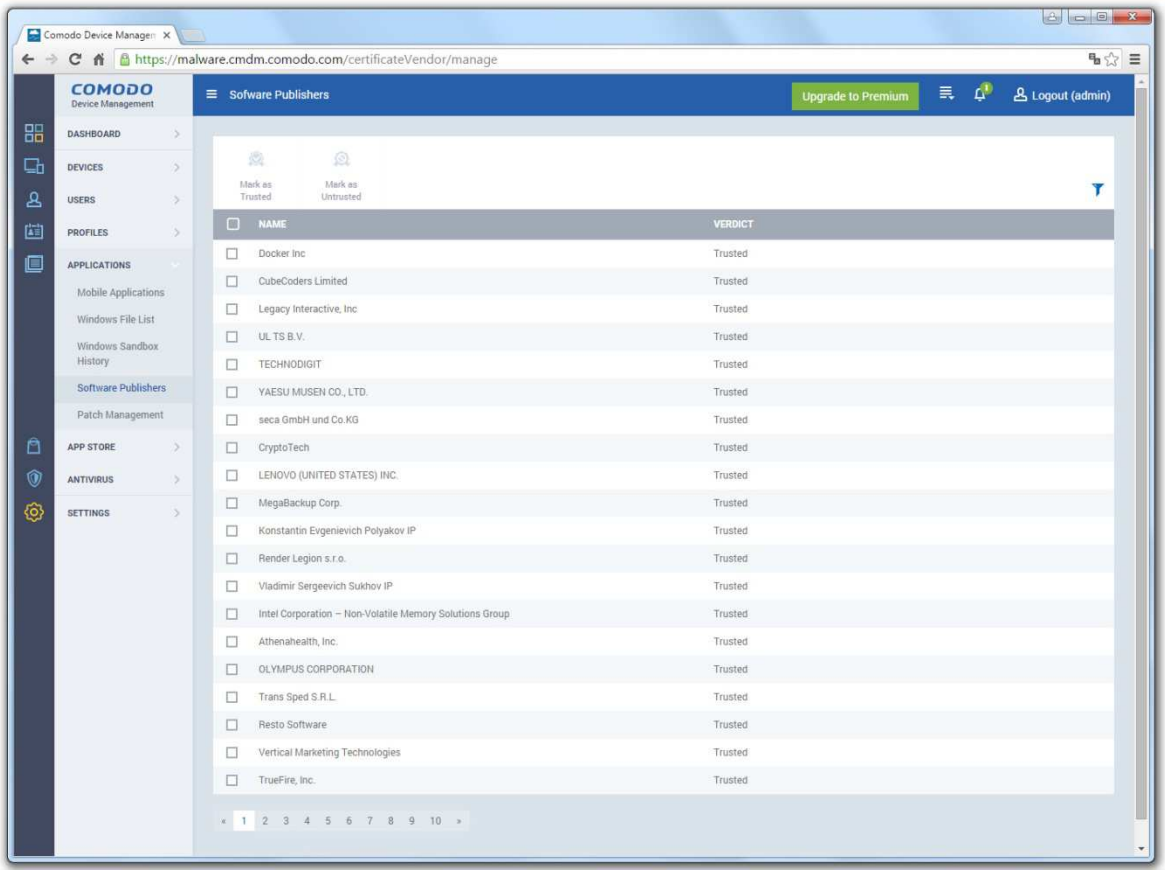
21. Aplikacje w automatycznej piaskownicy

Automatyczna piaskownica Comodo zwraca do konsoli wynik plików uruchomionych w bezpiecznym kontenerze.



22. Zaufani dostawcy

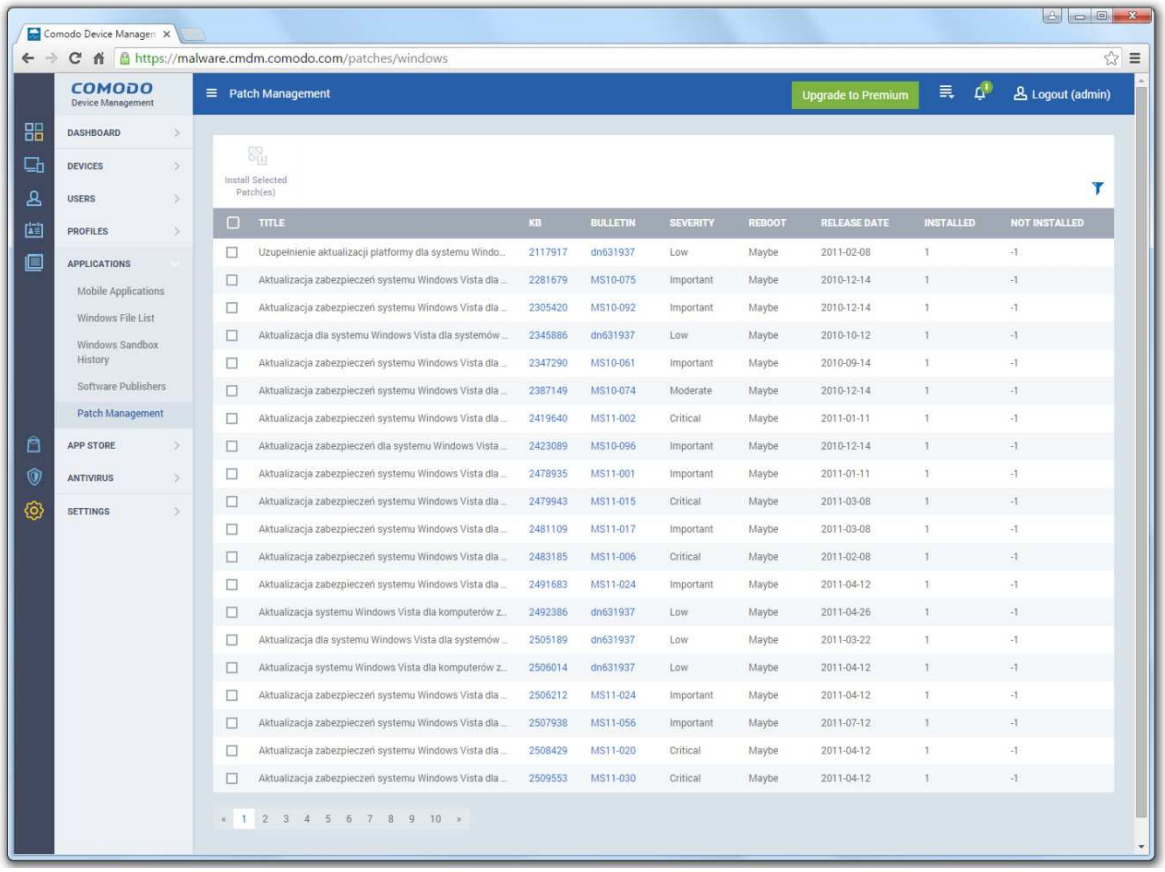
Zakładka Software Publisher zawiera listę wszystkich zaufanych dostawców oprogramowania. Lista ta zawiera tysiące pozycji i pozwala uniknąć fałszywych komunikatów oraz oznaczenia bezpiecznej aplikacji jako potencjalnie szkodliwej lub groźnej dla systemu operacyjnego.



23. Patch Manager

Ryzyko związane z lukami w zabezpieczeniach oprogramowania są często niedoceniane. Cyberprzestępcy mogą wykorzystać je do napisania exploitów oraz zainfekować systemy operacyjne, co umożliwi im kradzież poufnych danych firmowych.

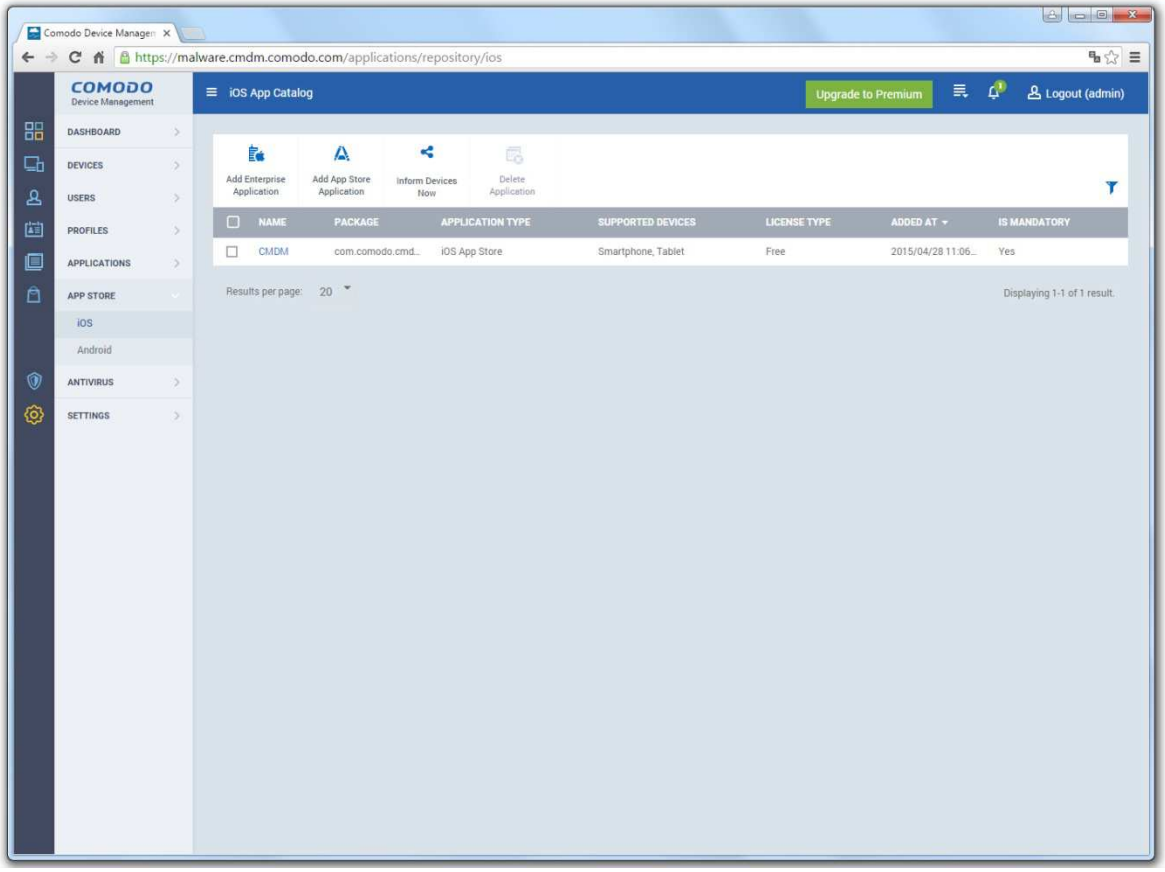
Funkcjonalność Patch Management zintegrowana z konsolą niweluje wektory ataków, które skierowane są w niezaktualizowane oprogramowanie i system Windows. Agent konsoli ITSM integrując się z urządzeniem wyszukuje brakujące łatki bezpieczeństwa w Windows Update oraz stare wersje aplikacji, takich jak Firefox, Chrome, Opera, oprogramowanie Adobe, Thunderbird i umożliwia ich aktualizację do najnowszej wersji bezpośrednio z konsoli CDM.



24. Kontrola urządzeń mobilnych

Produkt COMOD IT & Security Manager zawiera bogaty zestaw funkcji do zarządzania urządzeniami mobilnymi, które są własnością firmy lub pracownika.

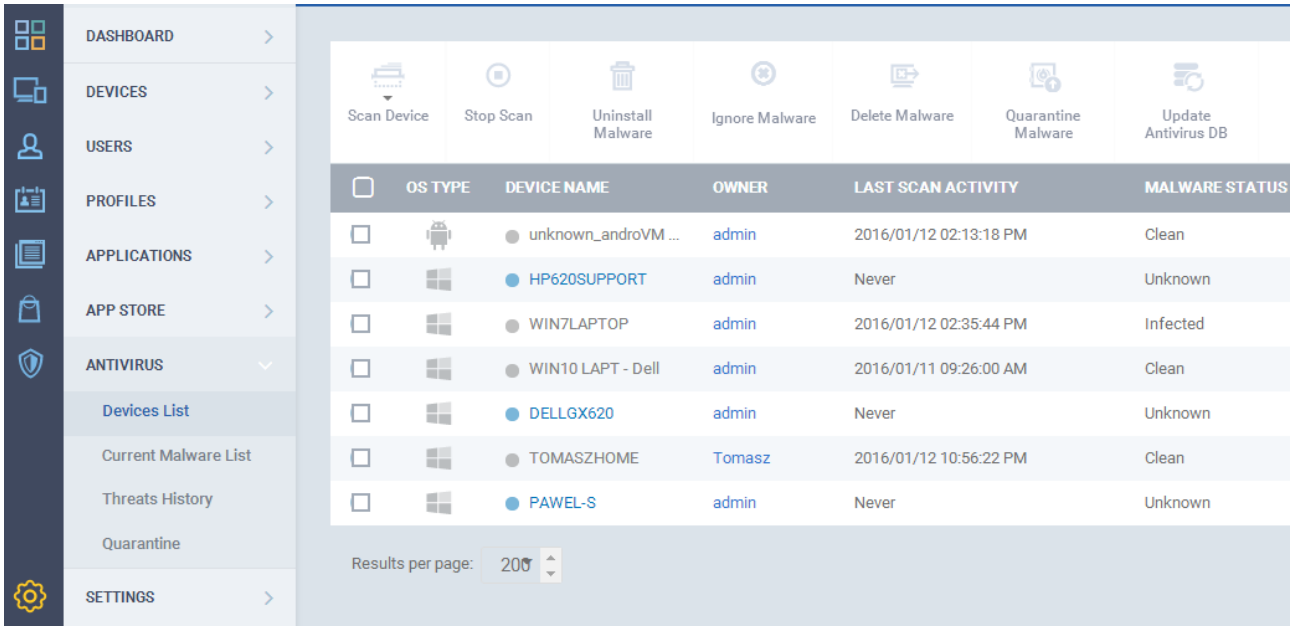
Zainstalowany agent w systemie iOS i Android daje możliwość śledzenia urządzenia (GPS), jak również wysłania powiadomień i instalowania rekomendowanych lub obowiązkowych aplikacji bezpośrednio ze sklepu App Store. Programy takie zostaną automatycznie usunięte z urządzenia po deinstalacji agenta.



25. Skanowanie i kontrola nad infekcjami

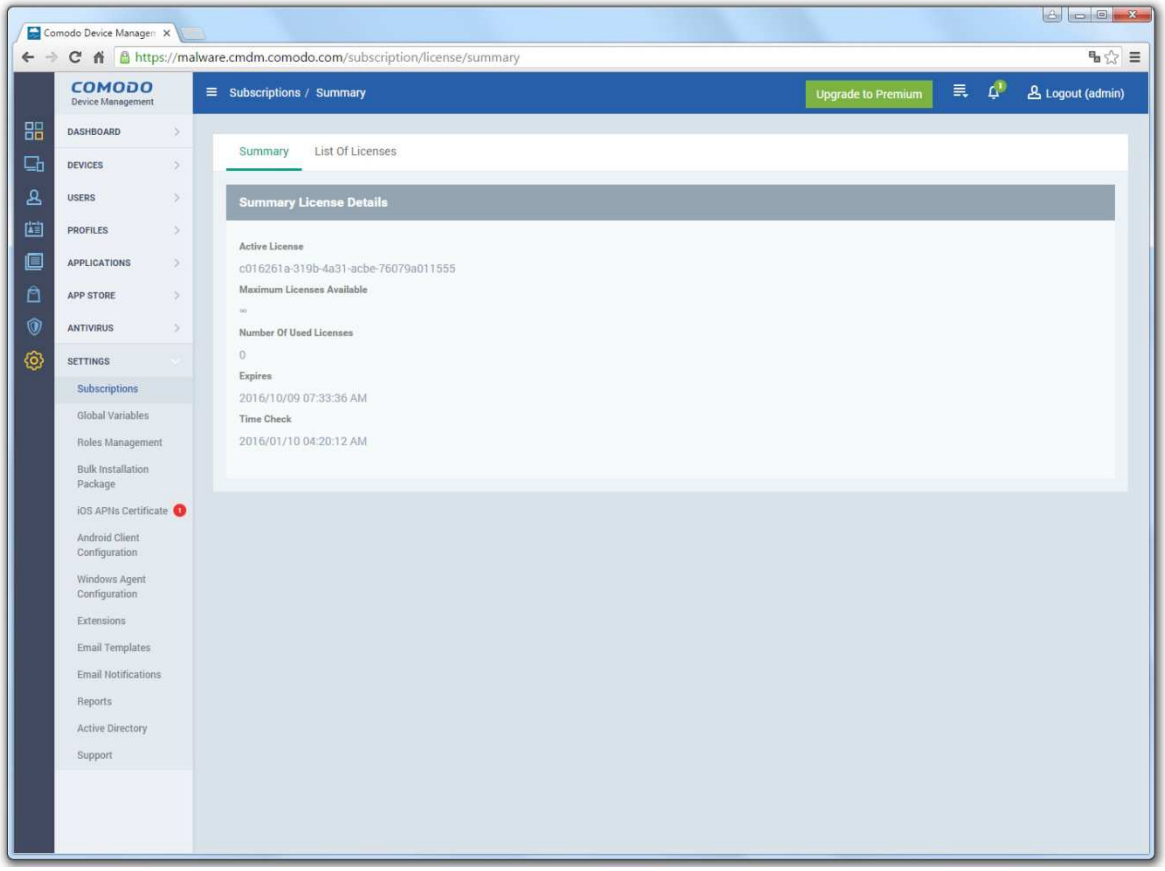
Poniższy screen przedstawia listę urządzeń, dla którym administrator może zdalnie wywołać komendę skanowania, usunąć zagrożenia, przenieść blokowane pliki do kwarantanny oraz zaktualizować bazy sygnatur wirusów.

- Komenda „odinstaluj malware” (Uninstall Malware)przeznaczona jest dla systemu Android.
- Komenda „usuń malware” (Delete Malware) dla systemów Windows.

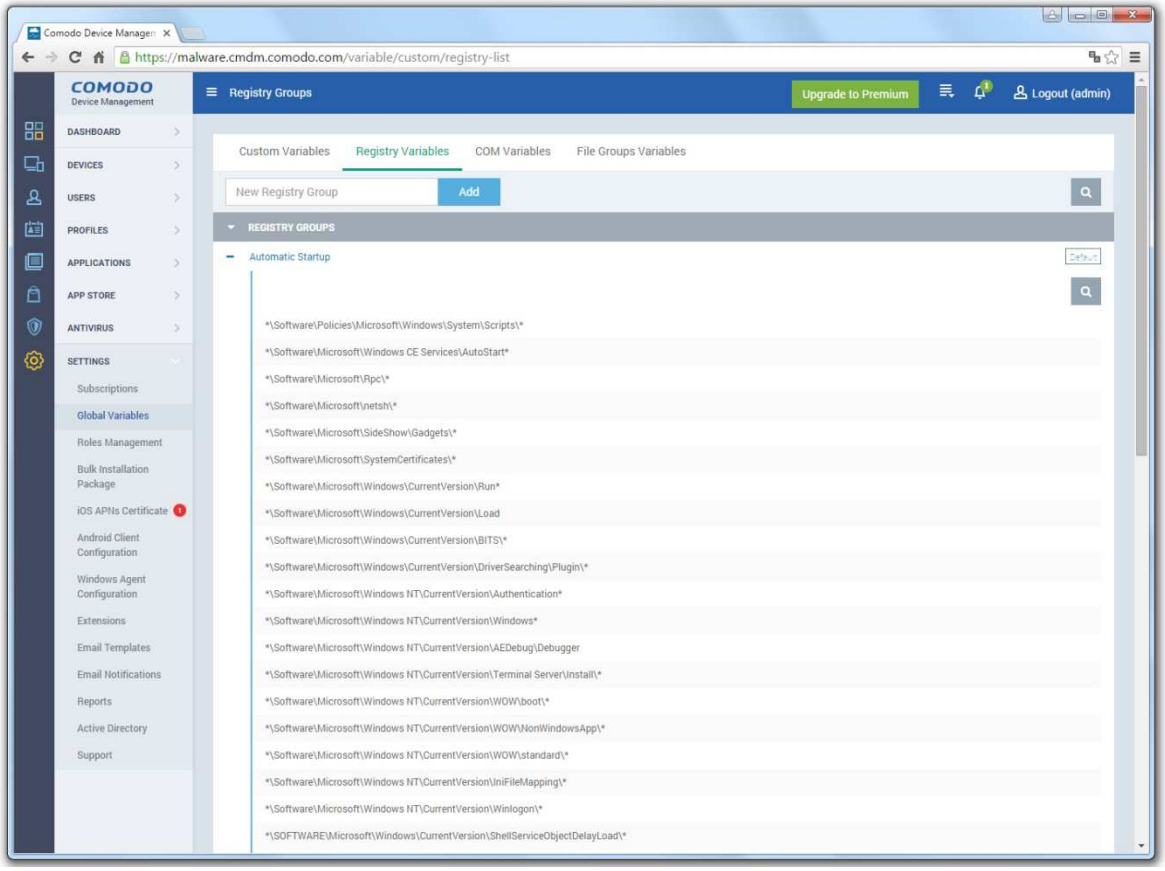


26. Informacje o licencji

W panelu tym znajdują się informacje o licencji użytkownika.



Konsola ITSM umożliwia administratorowi konfigurowanie zmiennych dla różnych ustawień profili bezpieczeństwa. Jako przykład, administrator może zdefiniować numer IMEI urządzenia, który będzie wykorzystywany przez inne aplikacje w telefonie.

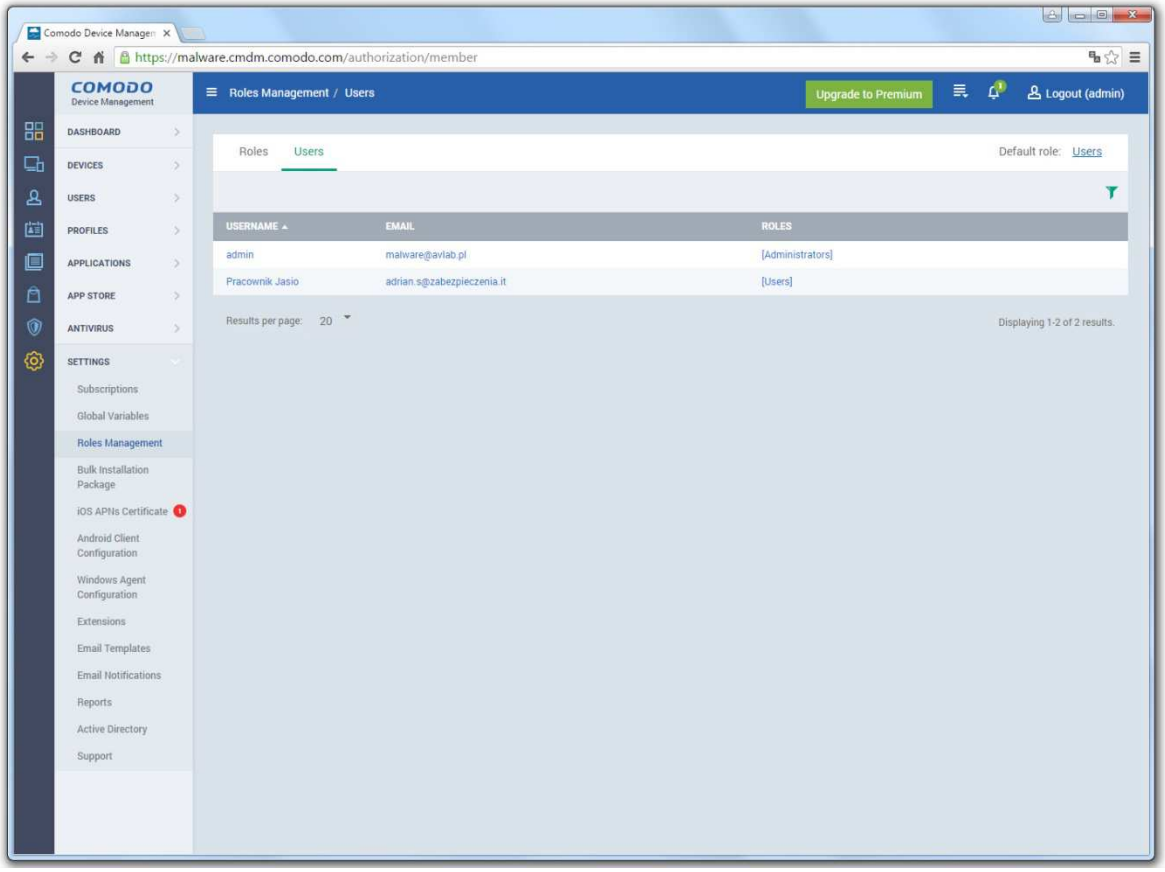


27. Zarządzanie konsolą uprawnienia

Administrator konsoli tworząc nowych użytkowników może przyznać im role:

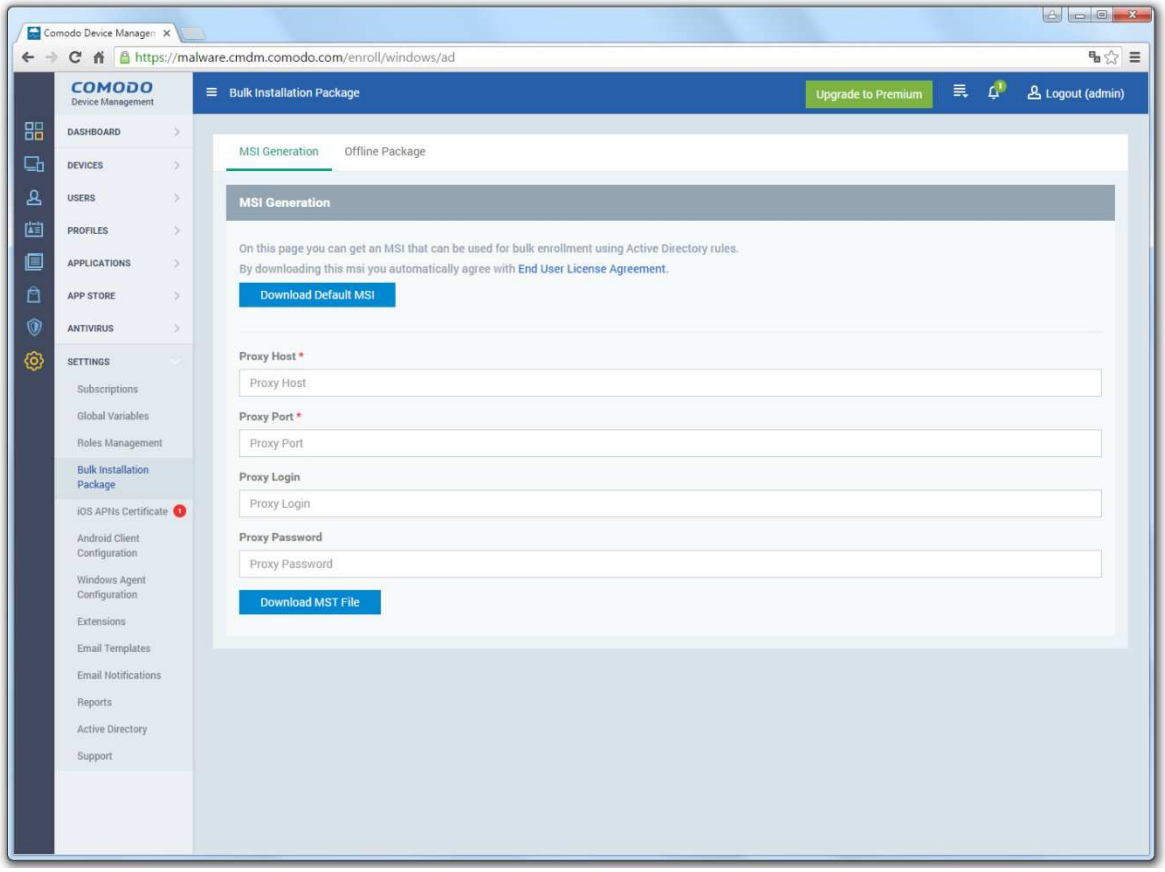
USER – użytkownik nie będzie w stanie uzyskać dostępu do konsoli, ale będzie mógł zarządzać swoim urządzeniem.

ADMIN – użytkownik o takich przywilejach będzie miał takie same uprawnienia, jak administrator główny, jednak nie będzie w stanie usunąć konta super administratora. Tworząc nowe konto z uprawnieniami administratora, użytkownik na adres e-mail otrzyma wiadomość, w jaki sposób zalogować się do konsoli.



28. Zarządzanie instalacją paczki MSI, Active Directry

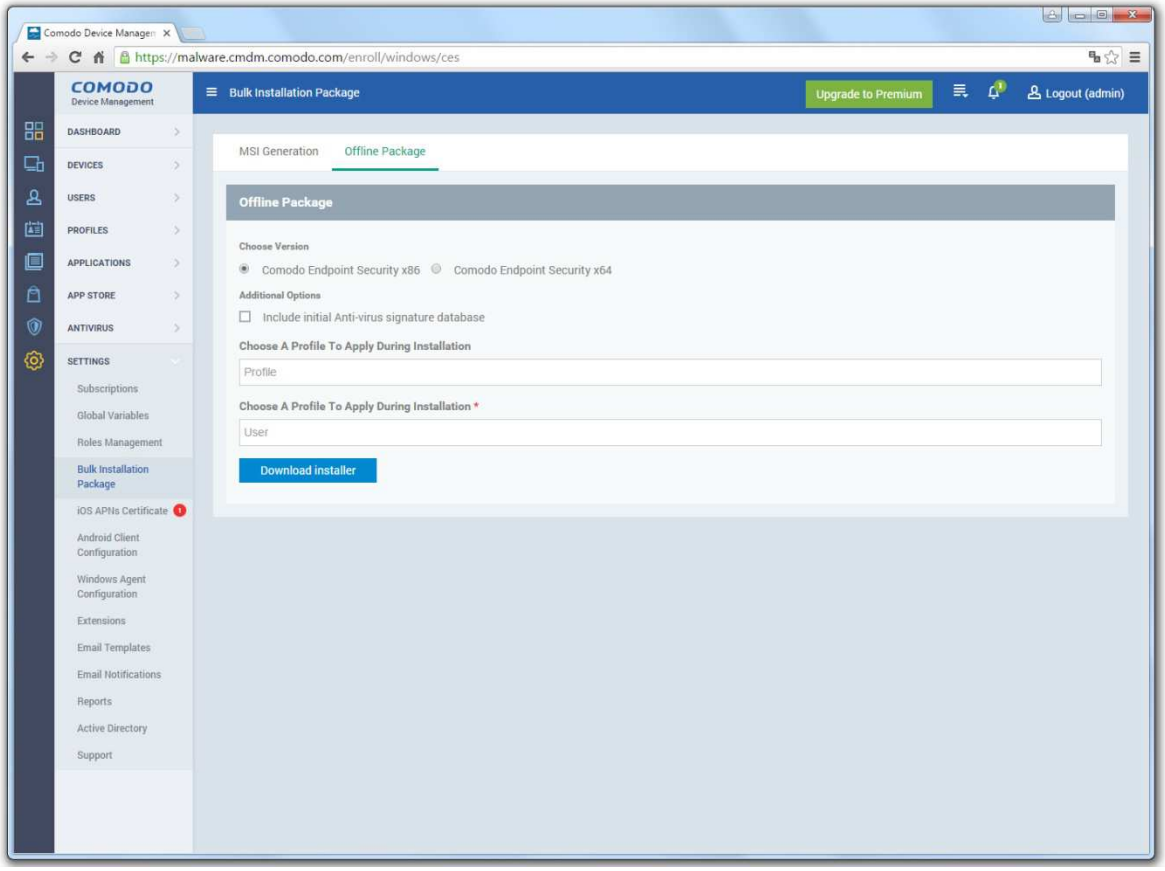
Na tej stronie administrator może pobrać paczkę MSI, aby wykorzystać ją do wdrożenia na wszystkich urządzeniach z systemem Windows, które znajdują się w usłudze katalogowej Active Directory.



29. Zarządzanie instalacją Offilne

Z poziomu tej zakładki administrator może pobrać wersję *offline* instalatora agenta konsoli wraz z agentem antywirusowym w jednym pliku MSI. Opcjonalnie, instalator może zawierać bazy sygnatur wirusów.

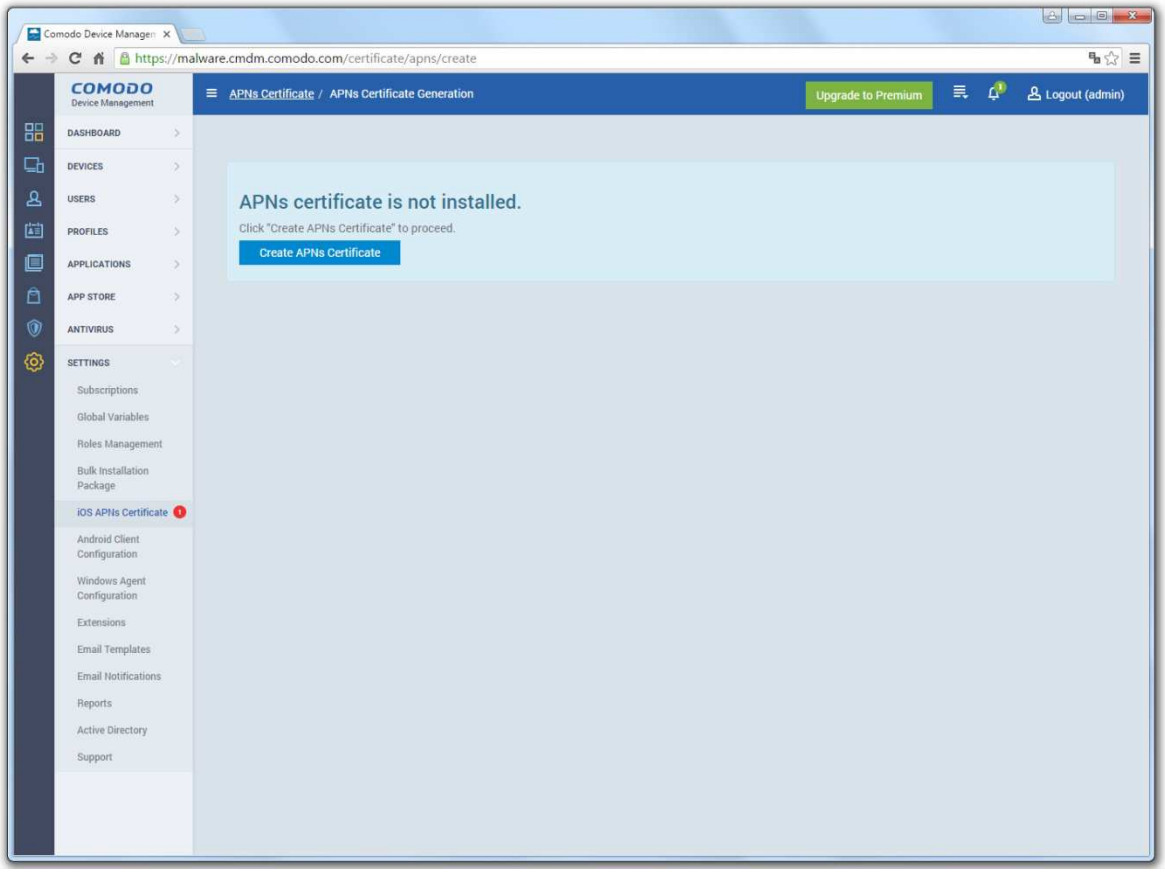
Plik MSI należy uruchomić na urządzeniu z uprawnieniami administratora.



30. Zarządzanie certyfikatami APN

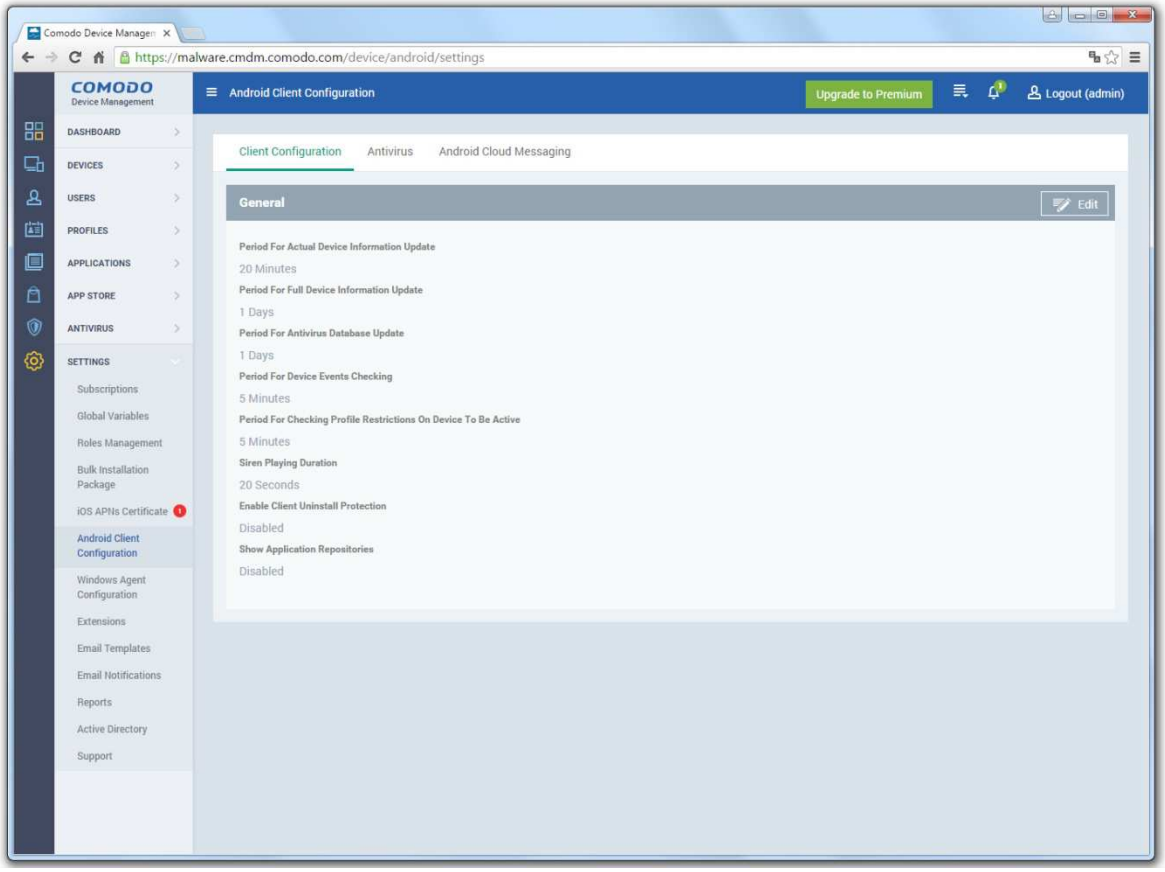
Konfiguracja certyfikatu APN (Apple Push Notofication) wymagana jest w celu ułatwienia komunikacji z zarządzanym urządzeniem z systemem operacyjnym iOS. Aby utworzyć taki certyfikat, należy postępować zgodnie z instrukcją, klikając w *Create APN's Certificate*.

Instrukcja dodania certyfikatu APN dostępna jest także na tej stronie.



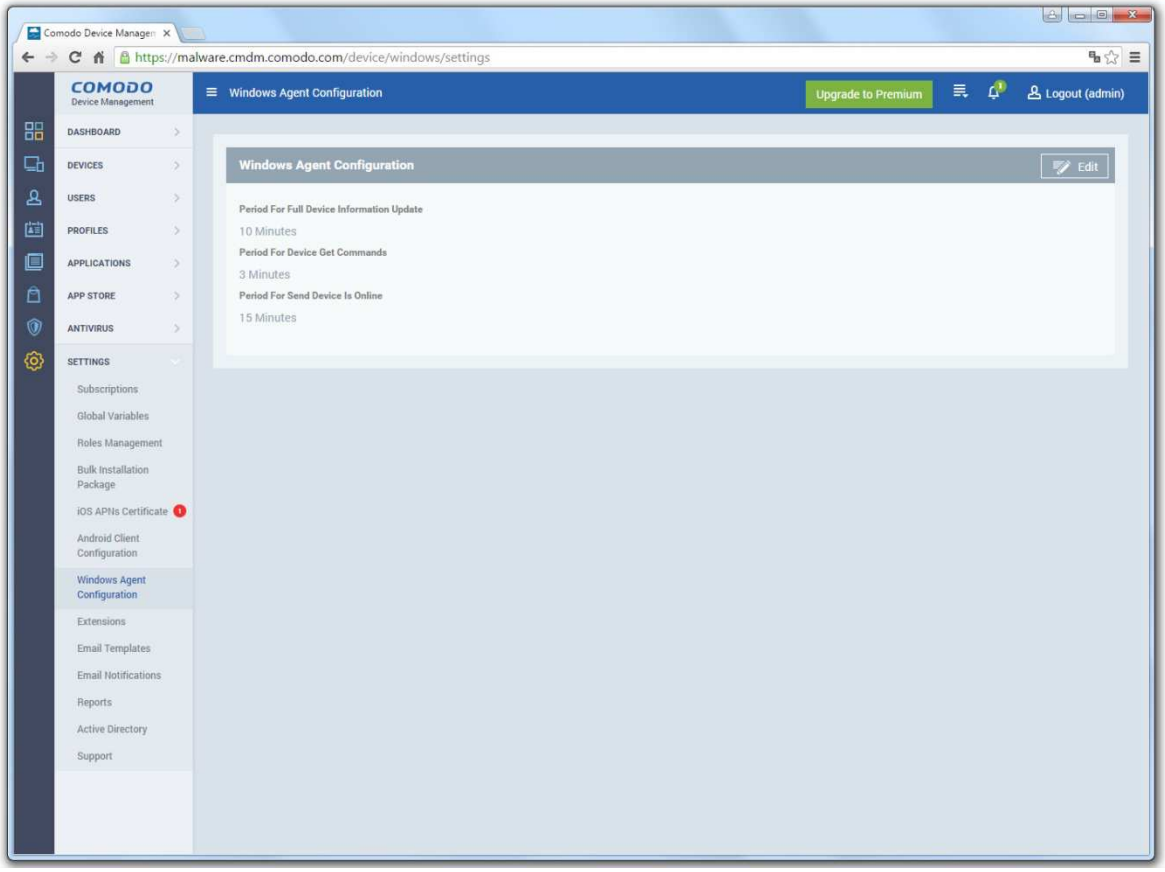
31. Android agent konfigurator

Konsola CDM pozwala administratorowi skonfigurować różne ustawienia, które zostaną wdrożone do agenta z systemem Android na zainstalowanym urządzeniu. W tym określić, po jakim czasie urządzenie będzie komunikowało się z konsolą, określić interwał pobierania sygnatur wirusów, pozwolić na manualne zarządzanie antywirusem pracownikowi.



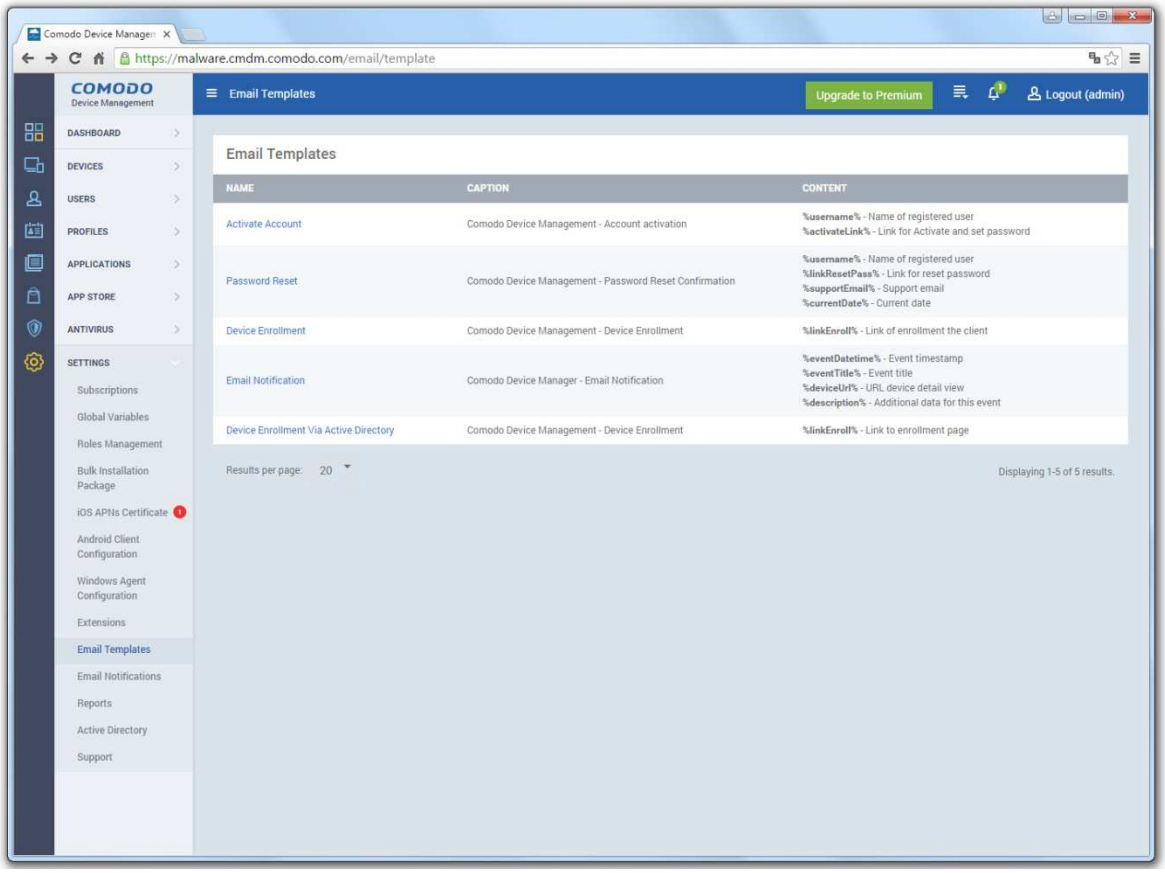
32. Windows agent konfigurator

Konsola ITSM pozwala administratorowi skonfigurować różne ustawienia, które zostaną wdrożone do agenta z systemem Windows. W tym: określić, po jakim czasie urządzenie będzie komunikowało się z konsolą wysyłając informacje o konfiguracji sprzętowej, oraz co ile minut będzie odbierało zdalne komendy wysłane z konsoli ITSM.



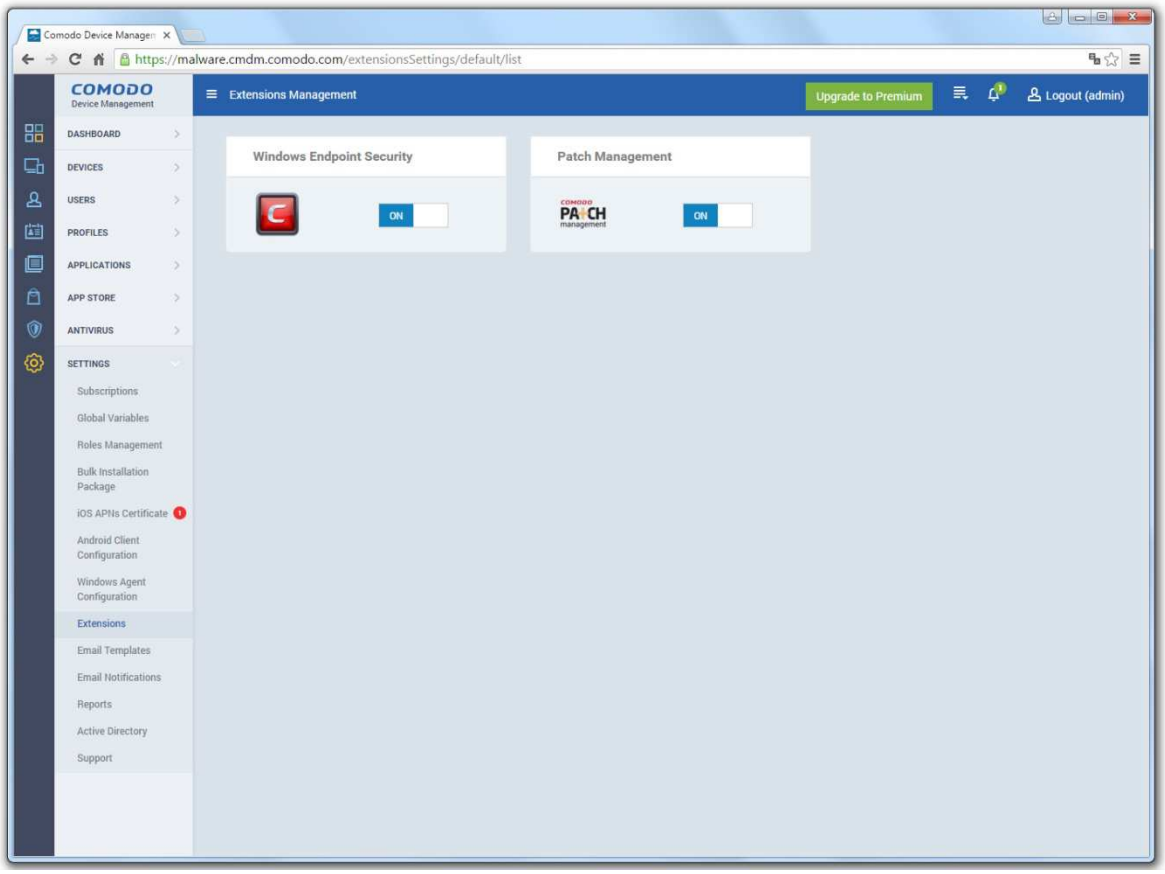
33. Powiadomienia e-mail kreator

Konsola ITSM wysyła kilka typów automatycznych powiadomień e-mail do użytkowników końcowych. Każdy szablon może być edytowany przez administratora, np. wstawiając własną treść w języku polskim dla łatwiejszego jej zrozumienia, np. aktywacja konta, zresetowanie hasło, wdrożenie agenta.



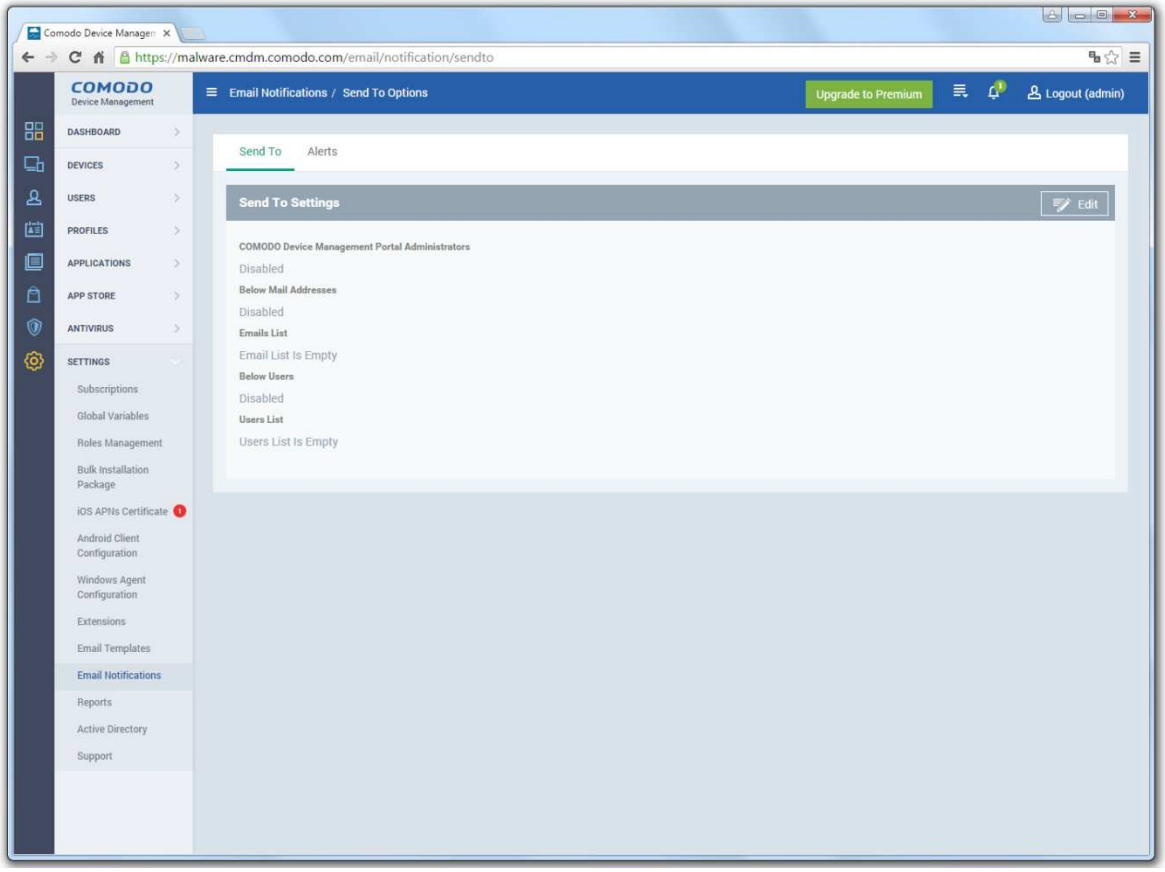
34. Zarządzanie aktualizacjami Windows Update i aplikacji trzecich

Konsola COMODO IT & Security Manager umożliwia nie tylko monitorowanie urządzeń, ale także ich ochronę oraz zarządzanie aktualizacjami Windows Update i aplikacji trzecich. Funkcjonalności te mogą być włączone lub wyłączone, w zależności od potrzeb przedsiębiorstwa.

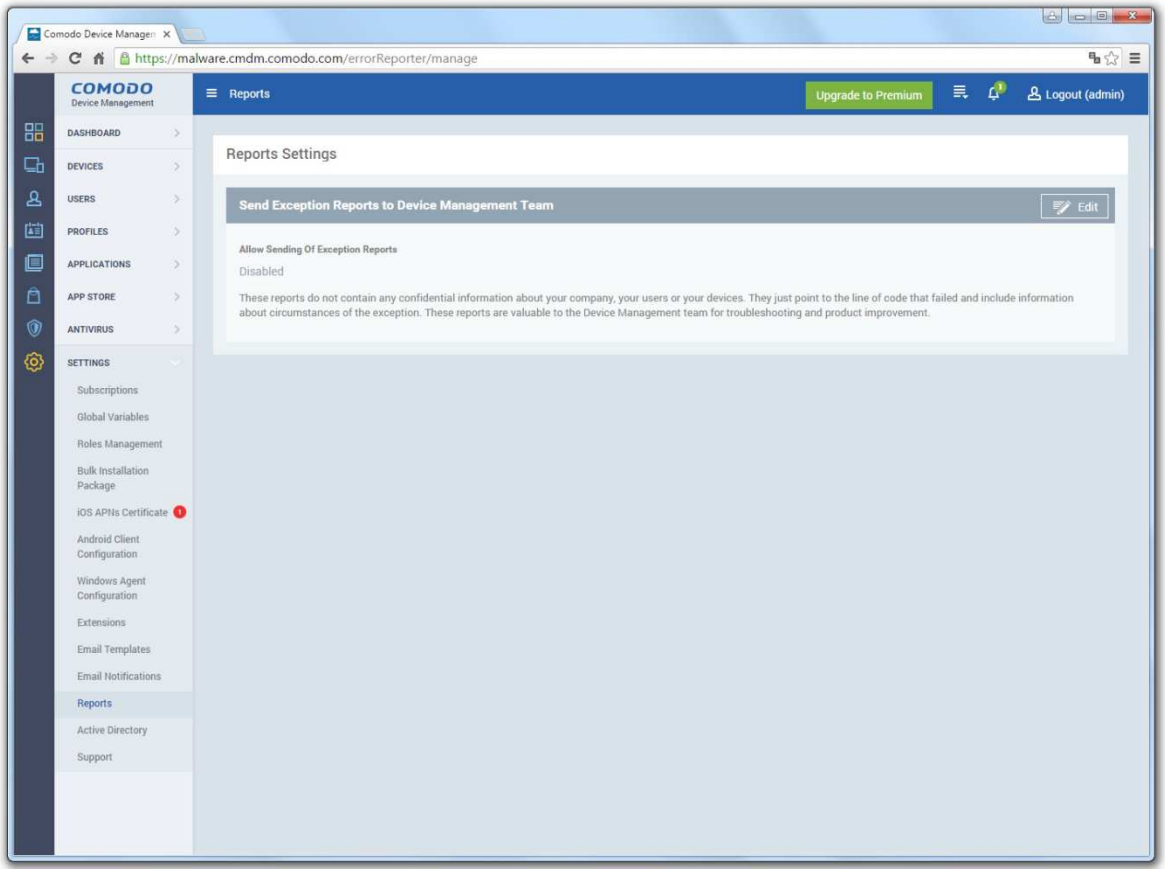


35. Zarządzanie wysyłanymi powiadomieniami

Administrator może wyświetlić pełne dane dotyczące powiadomień, które generowane są np. jeśli na urządzeniu w wyniku skanowania dostępowego zostanie zidentyfikowany złośliwy plik.



Administrator na podstawie informacji z urządzenia może wygenerować raport dotyczący inwentaryzacji sprzętu.



36. Pomoc techniczna producenta

W zakładce SUPPORT znajdują się informacje, dzięki którym możliwe jest uzyskanie pomocy technicznej bezpośrednio od producenta oraz informacje na temat wspieranych systemów operacyjnych dla urządzeń mobilnych i stacji roboczych.