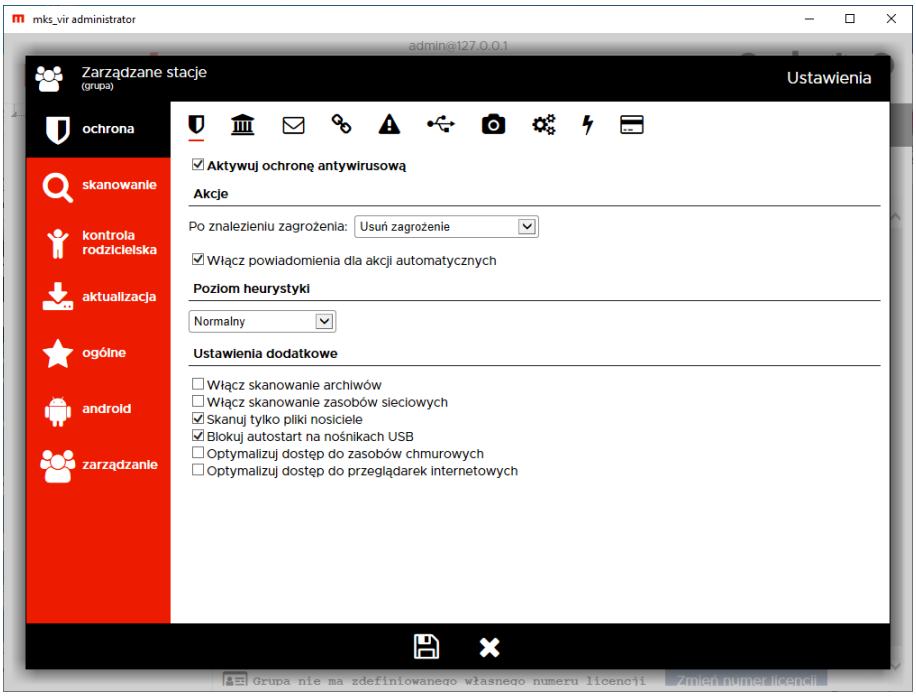
mks_vir administrator – szczegółowe ustawienia pakietu

Ustawienia szczegółowe pakietu **mks_vir** w konsoli administracyjnej dla grup lub stacji są identyczne

Ochrona → Ochrona plików:



Aktywuj ochronę antywirusową – opcja aktywuje najważniejszy moduł ochronny pakietu **mks_vir**

- **Po znalezieniu zagrożenia** – umożliwia wybranie akcji automatycznej, która ma być wykonana w przypadku znalezienia zagrożenia przez moduł ochrony antywirusowej; do wyboru są następujące możliwości:
  - **Usuń zagrożenie** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowany plik
  - **Skasuj plik** – kasuje zainfekowany plik
  - **Przenieś plik do kwarantanny** – przenosi zainfekowany plik do folderu kwarantanny **mks_vir**
  - **Blokuj dostęp** – blokuje zainfekowany plik, na skutek czego plik pozostaje na swoim miejscu, ale staje się niedostępny dla użytkownika
- **Włącz powiadomienia dla akcji automatycznych** – włącza wyświetlanie okien powiadomień modułu ochrony plików w przypadku znalezienia zagrożenia i wykonania wybranej akcji automatycznej

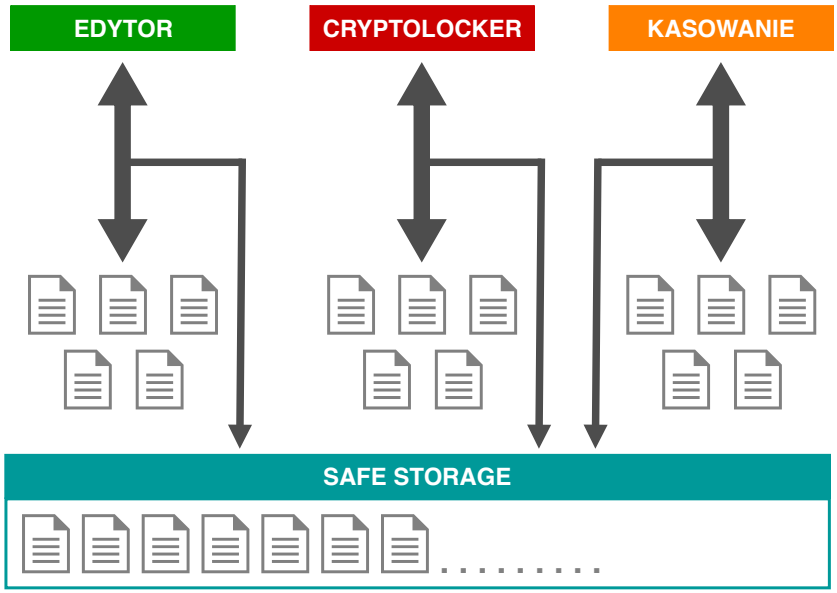
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia dodatkowe:

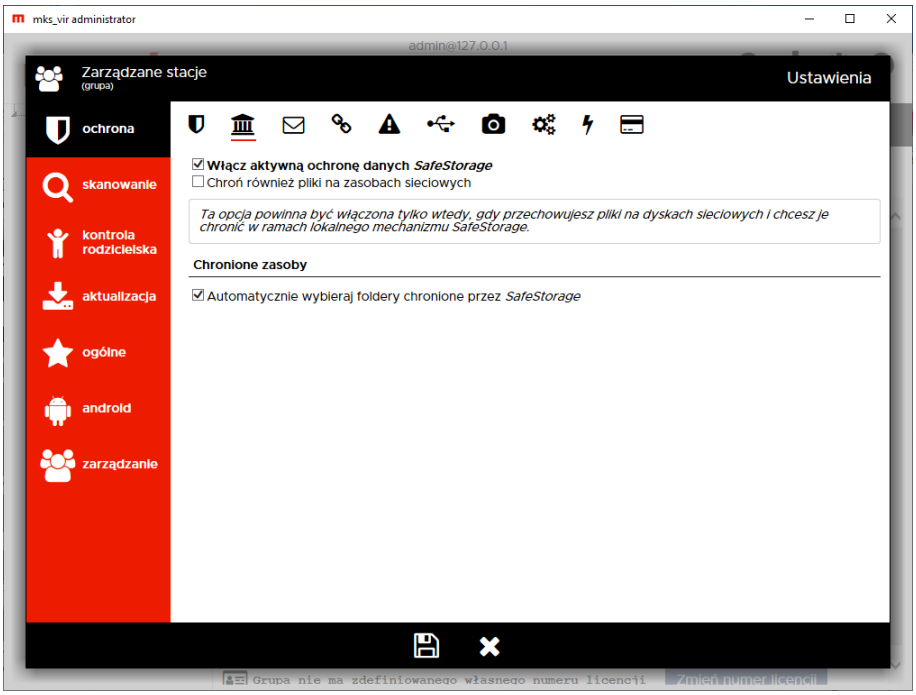
- **Włącz skanowanie archiwów** – włącza możliwość skanowania zawartości plików typu ZIP, RAR, 7Z itp.
- **Włącz skanowanie zasobów sieciowych** – włącza sprawdzanie podłączonych zasobów sieciowych; należy mieć na uwadze, że aktywność tej opcji może spowolnić dostęp do plików znajdujących się na podłączonych zasobach sieciowych
- **Skanuj tylko nosiciele** – opcja powoduje, że sprawdzane są tylko pliki będące domyślnymi nosicielami zagrożeń, jak np. pliki EXE, COM, JS, VBS itp.
- **Blokuj autostart na nośnikach USB** – uniemożliwia automatyczne uruchomienie z podłączanych pendrive potencjalnych zagrożeń
- **Optymalizuj dostęp do zasobów chmurowych** – optymalizuje skanowania obiektów przechowywanych w chmurze (np. Microsoft Onedrive, Google Drive itp.)
- **Optymalizuj dostęp do przeglądarek internetowych** – optymalizuje wydajność pracy przeglądarek internetowych (np. Microsoft Edge, Google Chrome itp.)

Ochrona → SafeStorage:

SafeStorage to nowatorska technologia pozwalająca na ochronę ważnych danych (różnego rodzaju dokumentów, plików graficznych, baz, arkuszy itp.) przed ich niepożądaną modyfikacją, zaszyfrowaniem, zniszczeniem lub skasowaniem przez szkodliwe oprogramowanie jak również przez przypadkowe działanie użytkownika.



SafeStorage przechowuje oryginalną zawartość dokumentów, zdjęć i innych ważnych plików użytkownika, niezależnie od tego, w jaki sposób są one modyfikowane lub kasowane.



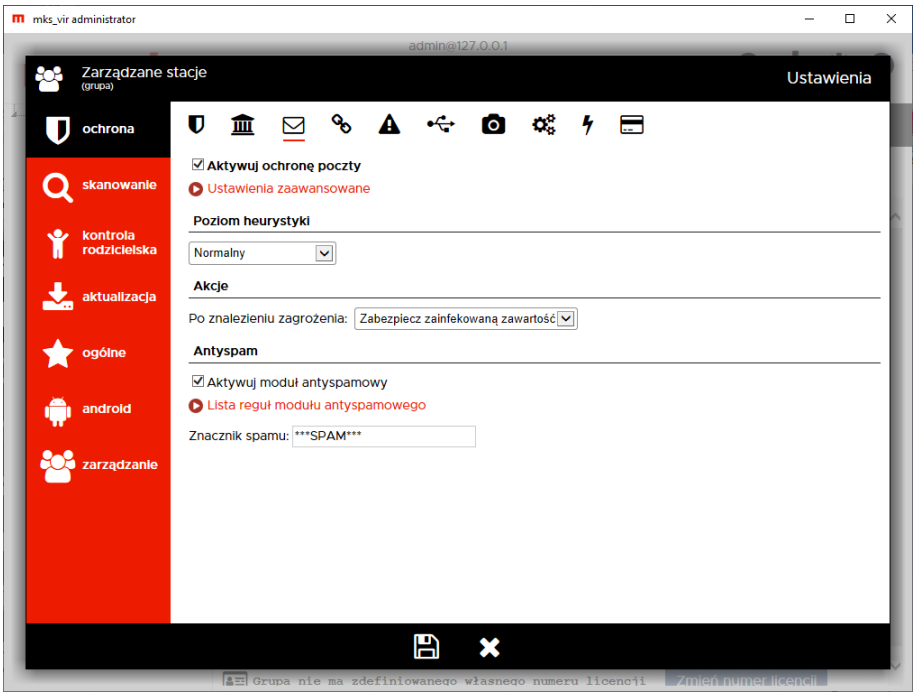
Włącz aktywną ochronę danych *SafeStorage* – włącza mechanizm ochrony danych, szczególnie przed zagrożeniami szyfrującymi (np. Cryptolocker)

- **Chroń również pliki na zasobach sieciowych** – włącza ochronę danych na podłączonych zasobach sieciowych

Chronione zasoby – pozwala na określenie, czy program ma automatycznie wybrać chronione lokalizacje, czy też ma je wskazać użytkownik

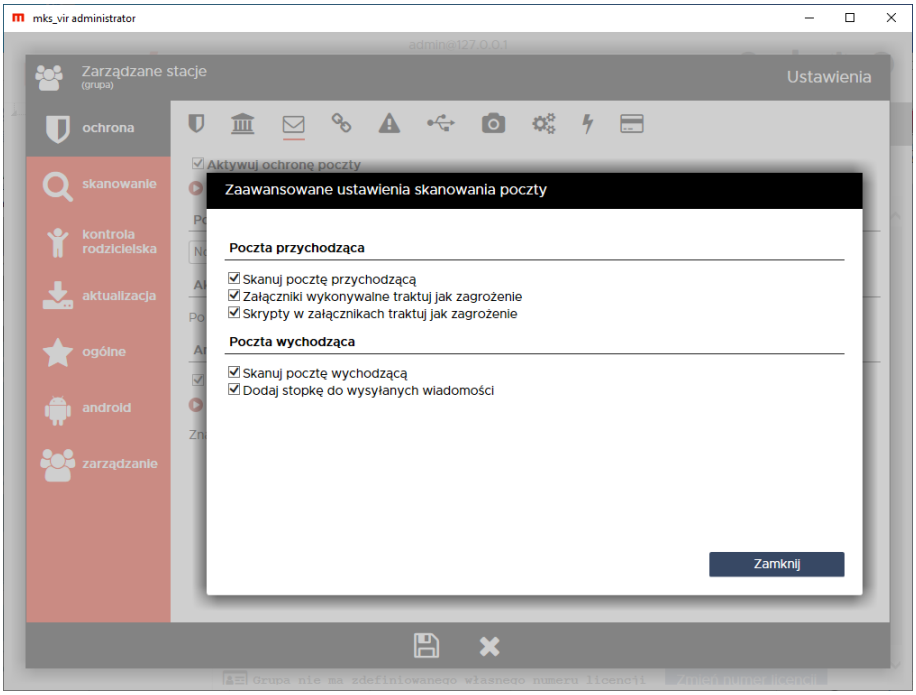
- **Automatycznie wybieraj foldery chronione przez *SafeStorage*** – przy włączonej opcji program domyślnie chroni dane na wszystkich dyskach lokalnych dostępnych w komputerze; jej wyłączenie umożliwia wybranie, które foldery mają być chronione

Ochrona → Ochrona poczty:



Aktywuj ochronę poczty – aktywuje moduł ochrony pobieranej i wysyłanej poczty; obsługiwane protokoły to POP3, IMAP i SMTP (w wersji zwykłej i szyfrowanej)

Ustawienia zaawansowane – umożliwiają dostrojenie ustawień dla pobieranej i wysyłanej poczty:



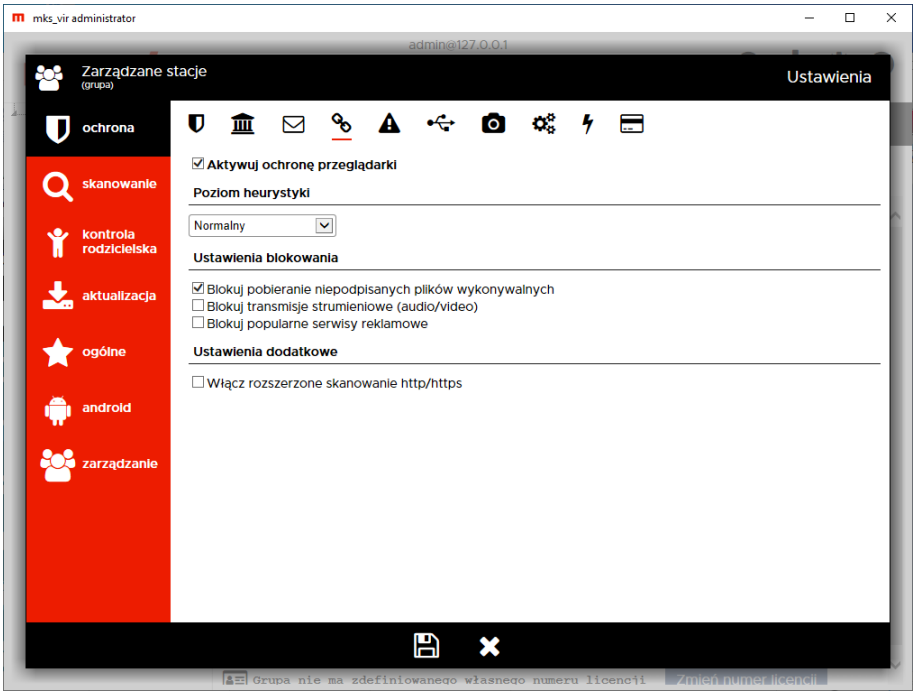
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Akcje – umożliwia wybranie automatycznej akcji, która ma być wykonana w przypadku znalezienia zagrożenia przez moduł ochrony poczty; do wyboru są następujące możliwości:

- **Zabezpiecz zainfekowaną zawartość** – zainfekowana wiadomość zostaje obudowana dla bezpieczeństwa - orginalny email znajduje się wtedy z załączniku takiej wiadomości
- **Usuń zainfekowaną zawartość** – zawartość email, będąca nośnikiem infekcji zostaje skasowana, zaś do odbiorcy zostaje dostarczona informacja o znalezionej infekcji

Antyspam – moduł do znakowania wiadomości-śmieci

Ochrona → Ochrona przeglądarki:



Aktywuj ochronę przeglądarki – aktywuje ochronę antywirusową dla przeglądarek; obsługiwane protokoły to HTTP i HTTPS

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

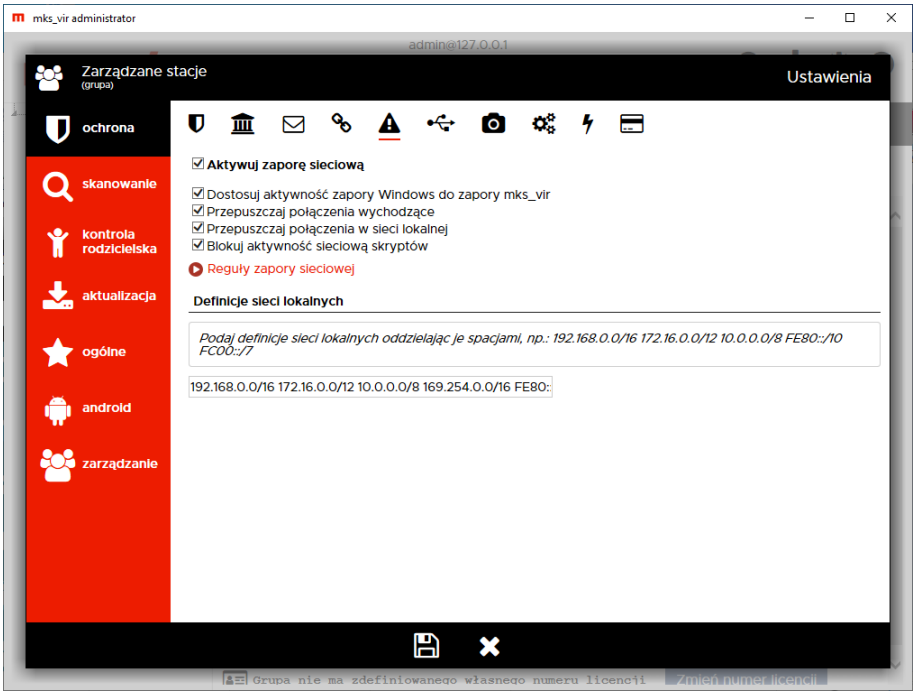
Ustawienia blokowania

- **Blokuj pobieranie niepodpisanych plików wykonywalnych** – włączenie tej opcji powoduje, że przy próbie pobrania niepodpisanych cyfrowo plików wykonywalnych (czyli takich, dla których nie da się automatycznie zweryfikować poprawności pochodzenia pliku), zostanie wyświetlone odpowiednie ostrzeżenie; użytkownik będzie mógł wtedy podjąć decyzję, czy dany plik pobrać, czy jednak nie
- **Blokuj transmisje strumieniowe (audio/video)** – włączenie tej opcji powoduje blokowanie wszelkiego rodzaju transmisji strumieniowych (co na przykład uniemożliwia słuchanie stacji radiowych przez internet)
- **Blokuj popularne serwisy reklamowe** – włączenie tej opcji powoduje blokowanie wyświetlania różnego rodzaju reklam pochodzących z najpopularniejszych serwisów reklamowych (włączenie opcji ***Włącz rozszerzone skanowanie http/https*** rozszerza zakres blokowanych reklam)

Ustawienia dodatkowe

- **Włącz rozszerzone skanowanie http/https** – włączenie tej opcji powoduje, że skanowane jest znacznie więcej elementów strumienia HTTP

Ochrona → Zapora sieciowa (firewall):



Aktywuj zaporę sieciową – aktywuje moduł ochrony sieci

- **Dostosuj aktywność zapory Windows do zapory mks_vir** – aktywność tej opcji umożliwia automatyczne przełączanie aktywności zapory Windows w zależności od aktywności *zapory mks_vir*; aktwacja *zapory mks_vir* wyłącza zaporę Windows, zaś dezaktywacja *zapory mks_vir* włącza zaporę Windows, dzięki czemu w systemie stale jest aktywna zapora
- **Przepuszczaj połączenia wychodzące** – dopuszcza wszystkie połączenia wychodzące; większość połączeń sieciowych, to połączenia wychodzące (np. typowa aktywność przeglądarki w czasie surfowania po internecie) i takie połączenia są w ogromnej większości bezpieczne
- **Przepuszczaj połączenia w sieci lokalnej** – aktywność tej opcji powoduje, że wszelkie połączenia nawiązywane w sieci lokalnej (połączenia wychodzące i przychodzące) są przepuszczane
- **Blokuj aktywność sieciową skryptów** – opcja ta blokuje możliwość łączenia się z różnymi witrynami lub pobierania plików, przez różnego rodzaju skrypty (JS, VBS itp.)

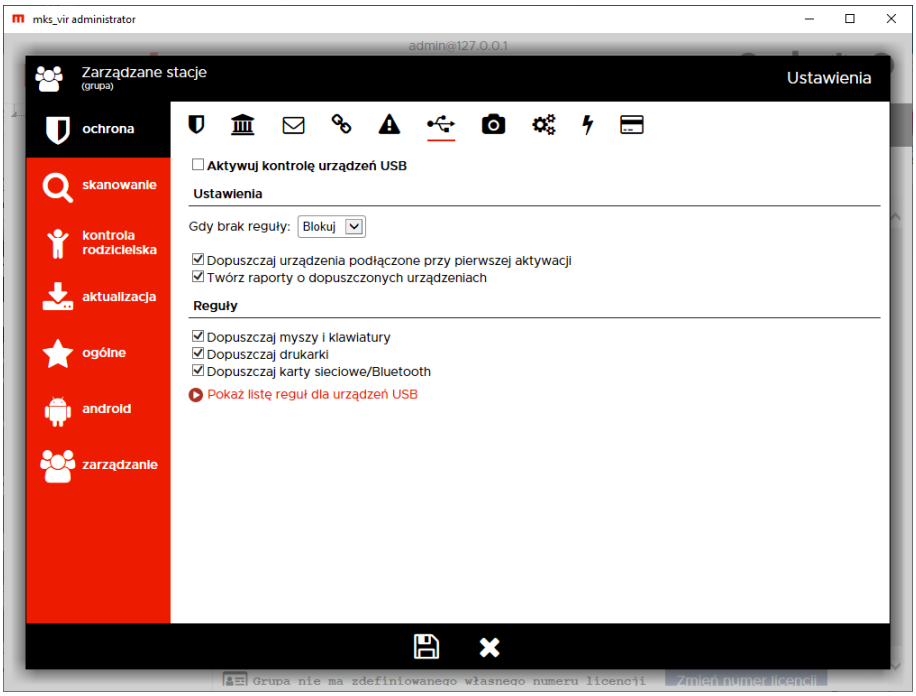
Reguły zapory sieciowej – umożliwia definiowanie własnych reguł przepuszczających lub blokujących ruch sieciowy różnych aplikacji

Definicje sieci lokalnych – domyślnie podane są tu standardowe definicje adresów i masek dla sieci lokalnych; jeśli używana jest inna definicja własnej sieci lokalnej, należy ją tu

podać, aby wszelkie reguły dotyczące sieci (w tym rozróżnienie – sieć lokalna czy nie) miały zastosowanie; definicje podajemy używając skróconego formatu maski, krótki opis jak korzystać z takich masek jest podany tu:

https://pl.wikipedia.org/wiki/Maska_podsieci

Ochrona → Kontrola urządzeń USB:



Aktywuj kontrolę urządzeń USB – aktywuje moduł kontroli urządzeń USB

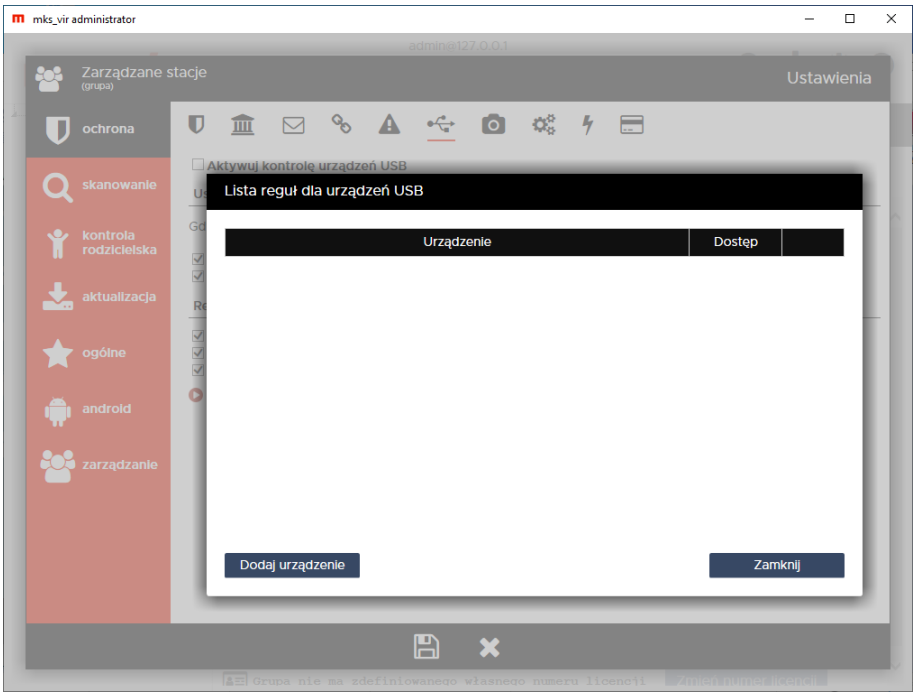
Ustawienia – umożliwia konfigurację modułu kontroli urządzeń USB

- **Gdy brak reguły** – umożliwia wybranie akcji, która ma być wykonana w przypadku podłączenia nowego urządzenia USB, czyli takiego dla którego nie jest zdefiniowana odpowiednia reguła (dopuszczająca lub blokująca); do wyboru są następujące możliwości:
  - **Blokuj** – blokuje każde nowe podłączane urządzenie USB
  - **Dopuść** – dopuszcza każde nowe podłączane urządzenie USB
- **Dopuszczaj urządzenia podłączone przy pierwszej aktywacji** – automatycznie dopuszcza urządzenia USB podłączone do komputera w momencie aktywacji modułu kontroli urządzeń USB
- **Twórz raporty o dopuszczonych urządzeniach** – włącza tworzenie raportów o podłączanych do komputera urządzeniach USB, dla których istnieją reguły dopuszczające lub wybraną akcją jest „Dopuść” (przy podłączaniu nowych urządzeń USB)

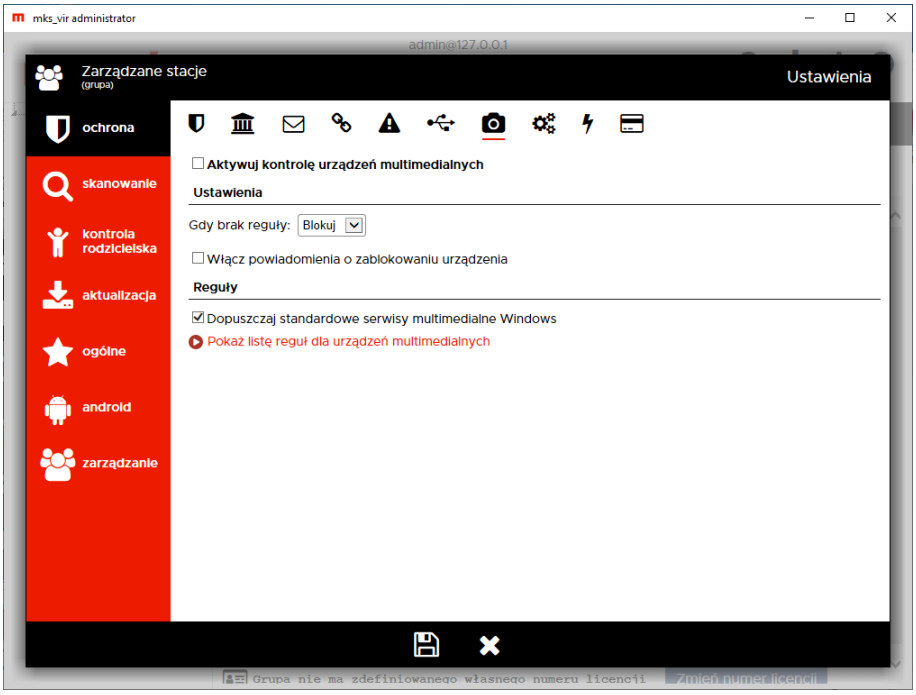
Reguły – umożliwia definiowanie lub modyfikację reguł blokujacych lub dopuszczajacych podłączane urządzenia USB

- **Dopuszczaj myszy i klawiatury** – automatycznie dopuszcza podłączane do komputera nowe klawiatury USB lub myszy USB
- **Dopuszczaj drukarki** – automatycznie dopuszcza podłączane do komputera nowe drukarki USB
- **Dopuszczaj karty sieciowe/Bluetooth** – automatycznie dopuszcza podłączane do komputera nowe karty sieciowe USB lub karty Bluetooth USB

Pokaż listę reguł dla urządzeń USB – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających dla podłączanych do komputera urządzeń USB:



Ochrona → Kontrola urządzeń multimedialnych:



Aktywuj kontrolę urządzeń multimedialnych – aktywuje moduł kontroli urządzeń multimedialnych

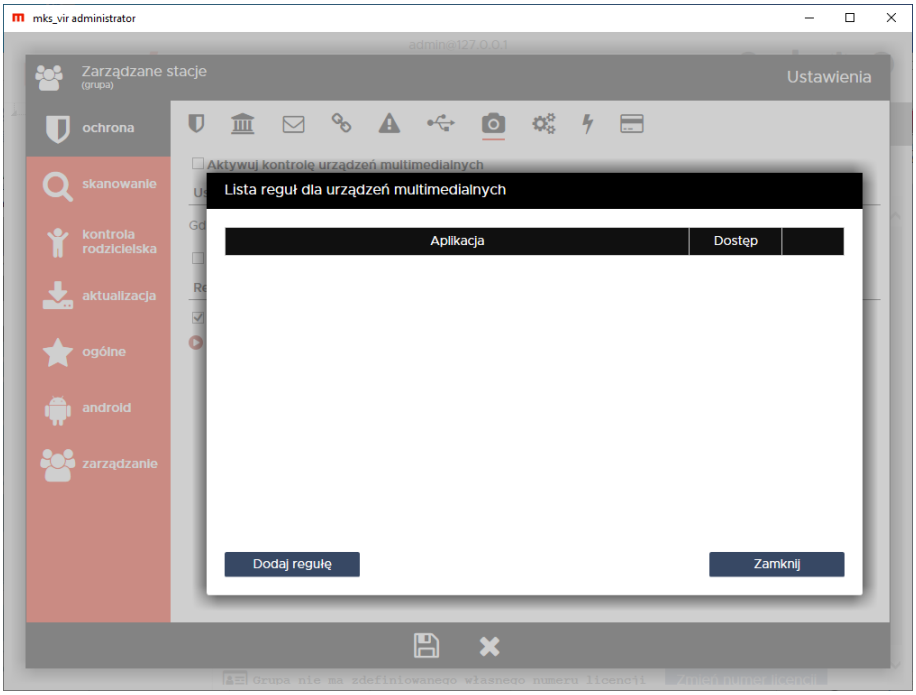
Ustawienia – umożliwia konfigurację modułu kontroli urządzeń multimedialnych

- **Gdy brak reguły** – umożliwia wybranie akcji, która ma być wykonana w przypadku próby dostępu do urządzenia multimedialnego przez aplikację, dla której nie jest zdefiniowana odpowiednia reguła (dopuszczająca lub blokująca); do wyboru są następujące możliwości:
  - **Blokuj** – blokuje próbę dostępu do urządzenia multimedialnego przez aplikację
  - **Dopuść** – dopuszcza próbę dostępu do urządzenia multimedialnego przez aplikację
- **Włącz powiadomienia o zablokowaniu urządzenia** – włącza wyświetlanie okien powiadomień modułu kontroli urządzeń multimedialnych w przypadku zablokowania dostępu do urządzenia multimedialnego przez aplikację na podstawie zdefiniowanej reguły lub w przypadku wybrania akcji automatycznej „Blokuj”

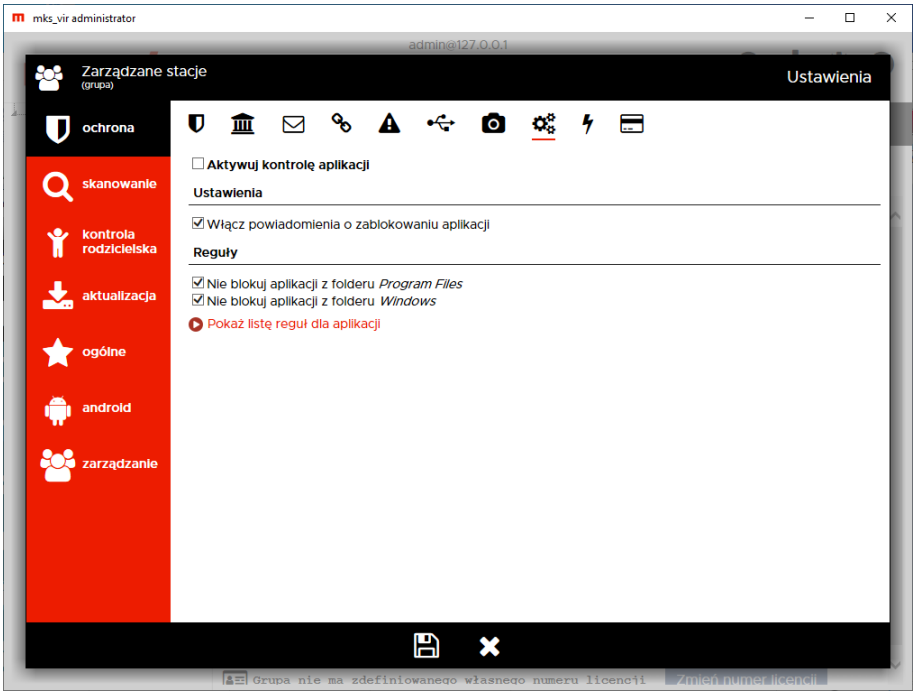
Reguły – umożliwia definiowanie lub modyfikację reguł blokujacych lub dopuszczajacych dostęp do urządzeń multimedialnych przez aplikacje

- **Dopuszczaj standardowe serwisy multimedialne Windows** – zezwala na dostęp do urządzeń multimedialnych systemowym serwisom obsługi takich urządzeń bez konieczności tworzenia odpowiednich reguł

Pokaż listę reguł dla urządzeń multimedialnych – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających dostęp do urządzeń multimedialnych przez aplikacje:



Ochrona → Kontrola aplikacji:



Aktywuj kontrolę aplikacji – aktywuje moduł kontroli aplikacji

Ustawienia – umożliwia konfigurację modułu kontroli aplikacji

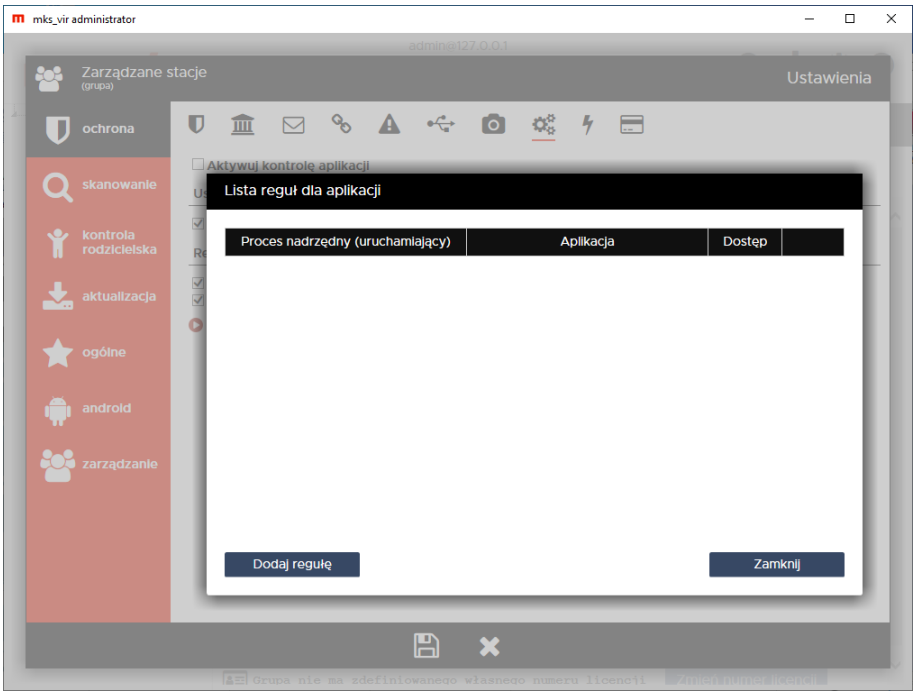
- **Włącz powiadomienia o zablokowaniu aplikacji** – włącza wyświetlanie okien powiadomień modułu kontroli aplikacji w przypadku zablokowania próby uruchomienia aplikacji, dla której została zdefiniowana reguła blokująca

Reguły – umożliwia definiowanie lub modyfikację reguł blokujacych lub dopuszczajacych uruchamianie aplikacji

- **Nie blokuj aplikacji z folderu *Program Files*** – wyklucza foldery systemowe *Program Files* i *Program Files (x86)* z obszaru działania zdefiniowanych przez użytkownika reguł blokujących
- **Nie blokuj aplikacji z folderu *Windows*** – wyklucza folder systemowy *Windows* z obszaru działania zdefiniowanych przez użytkownika reguł blokujących

> **Uwaga**: Nieodpowiednie reguły blokowania procesów przy wyłączonych opcjach dopuszczania aplikacji z folderów *Windows* i *Program Files* (czyli *Program Files* i *Program Files (x86)*) mogą doprowadzić do niestabilnej pracy systemu operacyjnego, a nawet uniemożliwić korzystanie z niego!

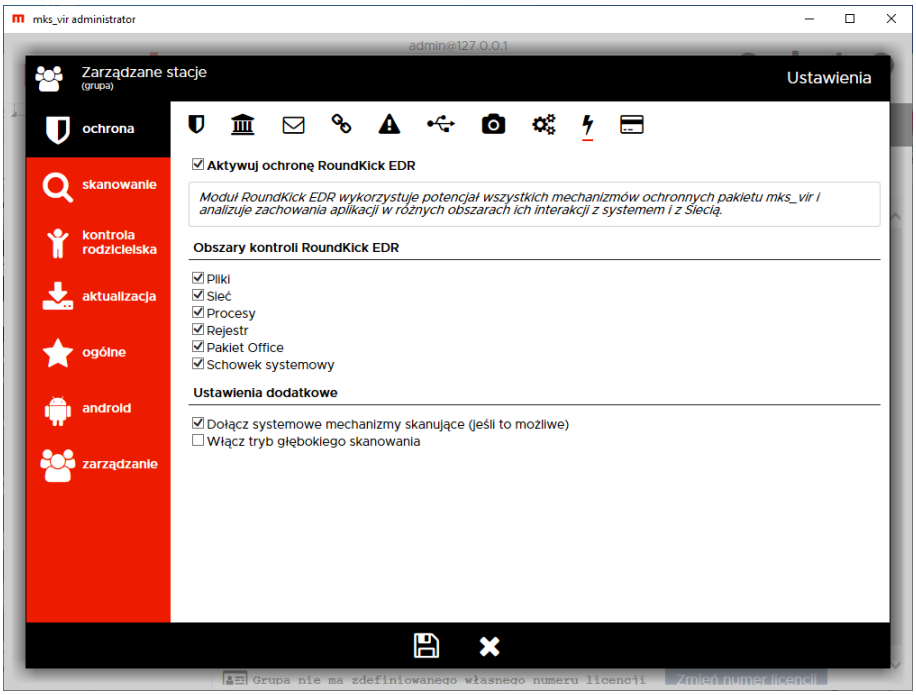
Pokaż listę reguł dla aplikacji – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających uruchamianie aplikacji:



Ochrona → Ochrona RoundKick EDR:

Moduł *RoundKick EDR* wykorzystuje potencjał wszystkich mechanizmów ochronnych pakietu **mks_vir** i analizuje zachowania aplikacji w różnych obszarach ich interakcji z systemem i siecią

Jego zadaniem jest wykorzystanie potencjału drzemiącego we wszystkich modułach ochronnych pakietu w procesie stałej analizy zachodzących w systemie zdarzeń. Mechanizm ten jest skonstruowany tak, aby nie zakłócał pracy użytkowników i nie generował fałszywych alarmów. Sytuacje podejrzane, ale nie wyczerpujące jeszcze w dostatecznym stopniu znamion cyberprzestępstwa, są delegowane do *chmury skanującej mks_vir*, w której podlegają procesom analizy automatycznej. Jeśli ta zawiedzie, do pracy siadają analitycy. Efektem może być odrzucenie zdarzenia jako nieszkodliwego, bądź natychmiastowa aktualizacja schematów i blokada szkodliwej aktywności.



Aktywuj ochronę RoundKick EDR – aktywuje moduł ochrony *RoundKick EDR*

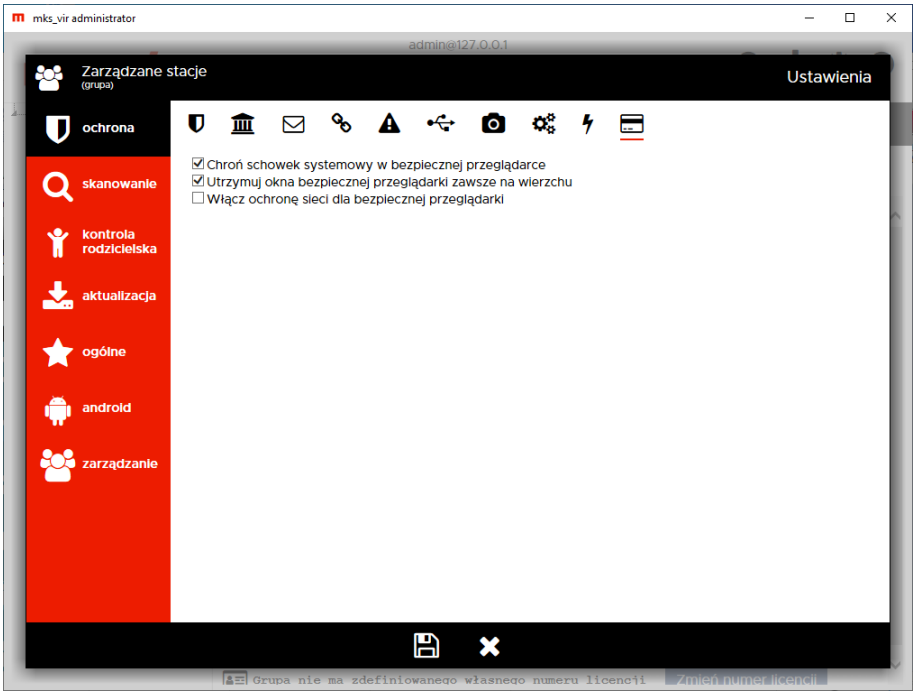
Obszary kontroli RoundKick EDR – pozwala na określenie w jakich zakresach mają być aktywne zaawansowane mechanizmy ochronne *RoundKick EDR*

- **Pliki** – kontroluje podejrzane zachowania i aktywności w systemie plików; wymaga aktywnego modułu ochrony plików – ***Ochrona plików***
- **Sieć** – kontroluje podejrzane zachowania i aktywności ruchu sieciowego; do pełnej funkcjonalności wymaga aktywnych modułów sieciowych – ***Ochrona poczty***, ***Ochrona przeglądarki***, ***Zapora sieciowa (firewall)***
- **Procesy** – kontroluje podejrzane zachowania i aktywności procesów w systemie operacyjnym
- **Rejestr** – kontroluje podejrzane modyfikacje rejestru systemowego; wymaga aktywnego modułu ochrony rejestru
- **Pakiet Office** – kontroluje podejrzane zachowania aplikacji pakietów *MS Office*, *Libre Office* itp.; do pełnej funkcjonalności wymaga aktywnego modułu sieciowego – ***Ochrona przeglądarki***
- **Schowek systemowy** – kontroluje zawartość schowka systemowego pod kątem obecności szkodliwych lub niebezpiecznych treści

Ustawienia dodatkowe – pozwalają na określenie jakie inne mechanizmy ochronne ma wykorzystywać program **mks_vir**

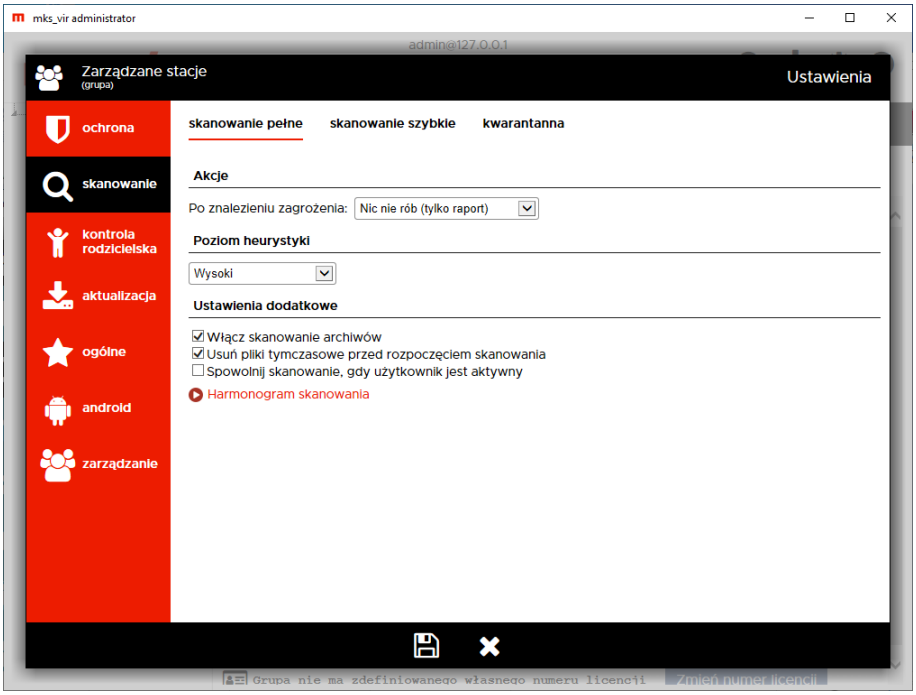
- **Dołącz systemowe mechanizmy skanujące (jeśli to możliwe)** – wyszukuje i wykorzystuje różne moduły skanujące, o ile jakieś są dostępne w systemie
- **Włącz tryb głębokiego skanowania** – włącza zaawansowane mechanizmy skanowania i emulacji celem dokładniejszej analizy skanowanych obiektów
  uwaga! włączenie opcji może powodować zauważalne wydłużenie czasów skanowania

Ochrona → Bezpieczna przeglądarka:



- **Chroń schowek systemowy w bezpiecznej przeglądarce** – włącza ochronę schowka systemowego przy aktywnej *bezpiecznej przeglądarce* programu **mks_vir** uniemożliwiając jego wykorzystanie we wszystkich aplikacjach (blokada operacji „Kopiuj → Wklej”, blokada „PrintScreen” itp.)
- **Utrzymuj okna bezpiecznej przeglądarki zawsze na wierzchu** – opcja ta przy pracy z *bezpieczną przeglądarką* programu **mks_vir** powoduje, że jej otwarte okna zawsze będą znajdowały się przed oknami innych, ew. otwartych aplikacji (tzw. *always on top*)
- **Włącz ochronę sieci dla bezpiecznej przeglądarki** – opcja ta przy pracy z *bezpieczną przeglądarką* programu **mks_vir** blokuje połączenia sieciowe realizowane przez wszystkie inne programy

Skanowanie → Skanowanie pełne:



Akcje – umożliwia wybranie akcji, która będzie wykonywania po zakończeniu pełnego skanowania komputera, do wyboru są następujące możliwości:

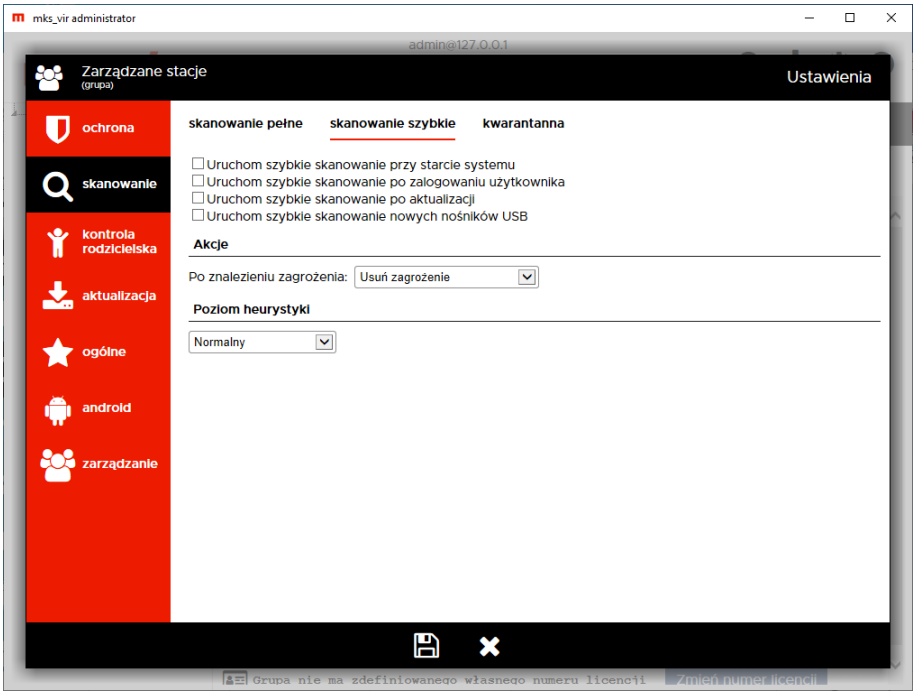
- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Nic nie rób (tylko raport)** – ew. znalezione w czasie skanowania zagrożenia pozostają tam gdzie były i tworzony jest tylko raport ze skanowania

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia dodatkowe:

- **Włącz skanowanie archiwów** – włącza możliwość skanowania zawartości plików typu ZIP, RAR, 7Z itp.
- **Usuń pliki tymczasowe przed rozpoczęciem skanowania** – usuwa pliki znajdujące się w folderach tymczasowych systemu i użytkowników przed rozpoczęciem skanowania
- **Spowolnij skanowanie, gdy użytkownik jest aktywny** – zwalnia szybkość skanowania, jeśli użytkownik w tym samym czasie wykonuje jakieś operacje
- **Harmonogram skanowania** – umożliwia określenie, kiedy ma się automatycznie rozpocząć skanowanie dysków komputera

Skanowanie → Skanowanie szybkie:



Skanowanie szybkie, które skanuje zawartość pamięci uruchomionych procesów i serwisów, może być automatycznie wykonywane w następujących przypadkach:

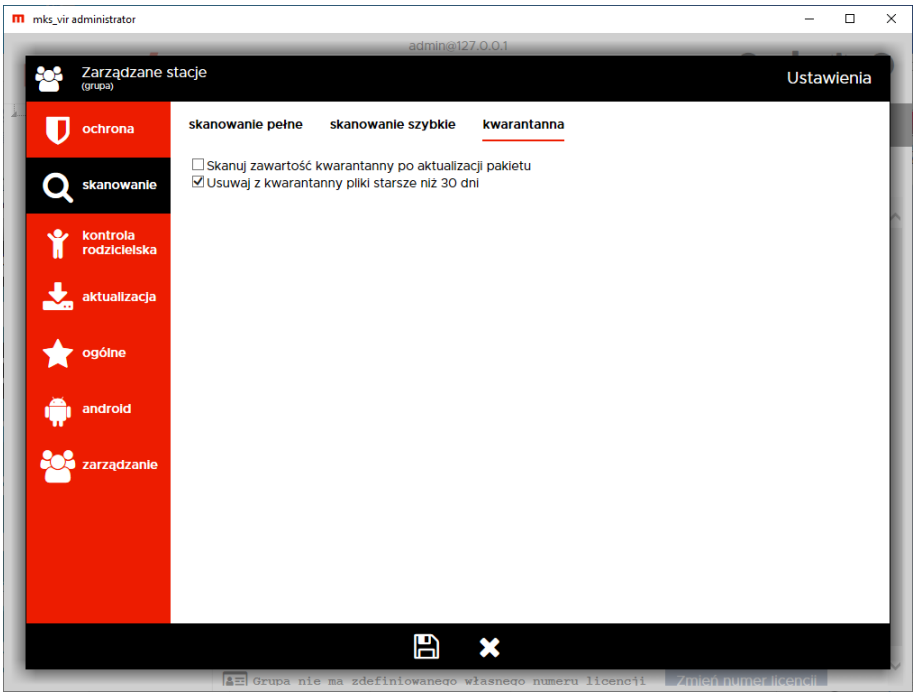
- **przy starcie systemu**
- **po zalogowaniu użytkownika**
- **po aktualizacji programu mks_vir**
- **po podłączeniu nośnika USB** – skanowana jest wtedy zawartość takiego nośnika

Akcje – umożliwia wybranie akcji, która będzie wykonywania po znalezieniu zagrożenia w czasie szybkiego skanowania, do wyboru są następujące możliwości:

- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Nic nie rób (tylko raport)** – ew. znalezione w czasie skanowania zagrożenia pozostają tam gdzie były i tworzony jest tylko raport ze skanowania

Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

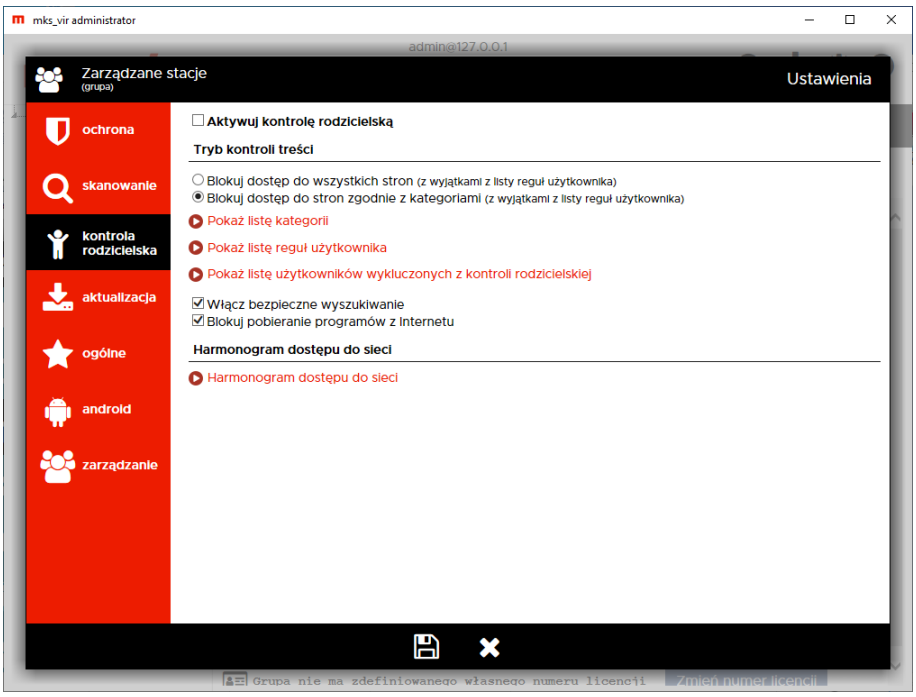
Skanowanie → Kwarantanna:



Automatyczne skanowanie i czyszczenie ze starych plików **kwarantanny** programu **mks_vir**:

- **Skanuj zawartość kwarantanny po aktualizacji pakietu** – automatycznie skanuje po zakończeniu aktualizacji pakietu pliki w kwarantannie, o ile oczywiście znajdują się tam jakiekolwiek pliki
- **Usuwaj z kwarantanny pliki starsze niż 30 dni** – automatycznie kasuje z kwarantanny pliki, które bez zmiany ich statusu (zmiana nazwy zagrożenia czy eliminacja tzw. „fałszywego alarmu”) znajdują się w niej dłużej niż 30 dni

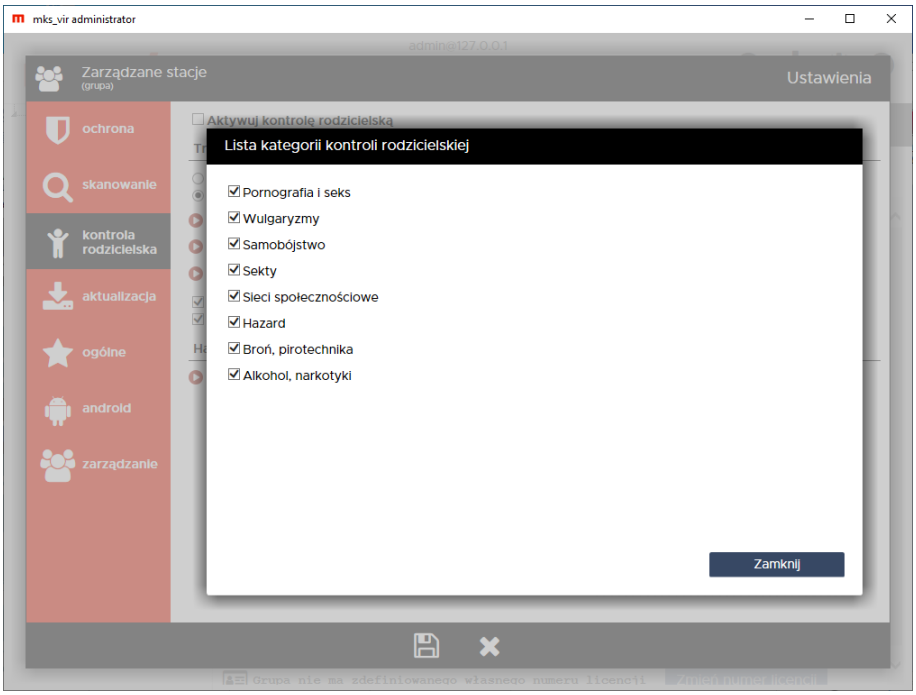
Kontrola rodzicielska:



Aktywuj kontrolę rodzicielską – uaktywnia moduł kontroli rodzicielskiej

Tryb kontroli treści – umożliwia określenie sposobu działania modułu kontroli rodzicielskiej:

- **Blokuj dostęp do wszystkich stron** – w tym trybie blokowane będą wszystkie strony internetowe, za wyjątkiem tych podanych w regułach użytkownika
- **Blokuj dostęp do stron zgodnie z kategoriami** – w tym trybie strony będą blokowane lub przepuszczane zależnie od analizy zawartości stron zgodnie z regułami zdefiniowanymi dla poszczególnych kategorii, aktywność poszczególnych kategorii można zmieniać po wybraniu „Pokaż listę kategorii”:



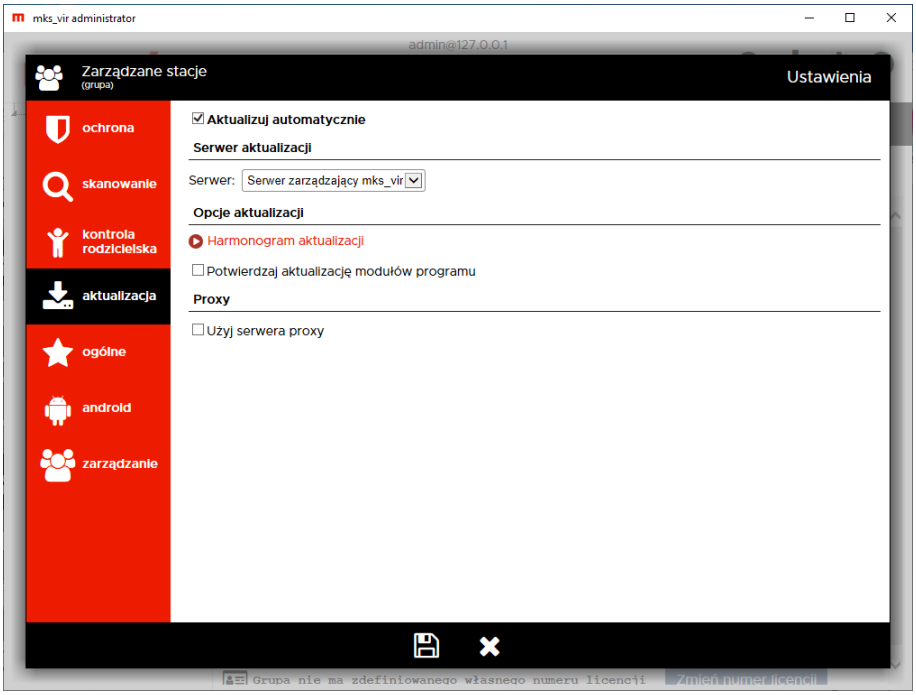
Pokaż listę reguł użytkownika – umożliwia zdefiniowane własnych reguł przepuszczających lub blokujących w oparciu o adresy lub frazy (słowa kluczowe)

Pokaż listę użytkowników wykluczonych z kontroli rodzicielskiej – umożliwia określenie użytkowników, dla których kontrola rodzicielska będzie zawsze nieaktywna

- **Włącz bezpieczne wyszukiwanie** – wymusza włączenie trybu bezpiecznego wyszukiwania (*SafeSearch*) w wyszukiwarkach
- **Blokuj pobieranie programów z Internetu** – uniemożliwia pobieranie programów z witryn internetowych

Harmonogram dostępu do sieci – umożliwia określenie, kiedy użytkownicy mają mieć dostęp do Internetu, a kiedy nie; aktywność tej opcji nie ma wpływu na dostępność zasobów w sieciach lokalnych

Aktualizacja:



Aktualizuj automatycznie – wymusza sprawdzanie co jakiś czas (jest on określany częściowo losowo w granicach kilkudziesięciu minut) dostępności aktualizacji i przy ich dostępności aktualizuje program **mks_vir**

Serwer – umożliwia wybranie źródła aktualizacji, do wyboru są następujące możliwości:

- **Serwer zarządzający mks_vir** – aktualizacje odbywają się z repozytorium tworzonego, aktualizowanego i udostępnianego automatycznie przez moduł **mks_vir administrator**
- **Inny serwer HTTP** – aktualizacje będą się odbywały z udostępnionego za pomocą protokołu HTTP repozytorium (np. tworzonego, aktualizowanego i udostępnianego przez program **mks_vir** nie zarządzany z poziomu programu **mks_vir administrator**)
- **Zasób lokalny** – aktualizacje będą się odbywały z repozytorium dostępnego na lokalnym nośniku, np. na pendrive; opcja może mieć znaczenie dla sieci całkowicie odciętych od Internetu

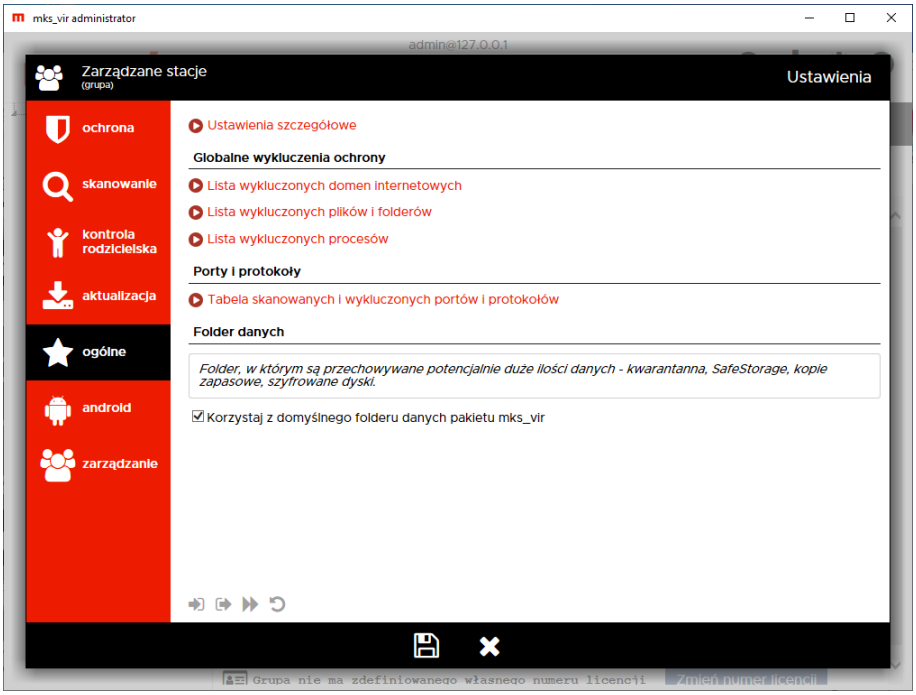
Opcje aktualizacji:

Harmonogram aktualizacji – umożliwia określenie, kiedy ma być bezwzględnie wymuszana aktualizacja programu **mks_vir**

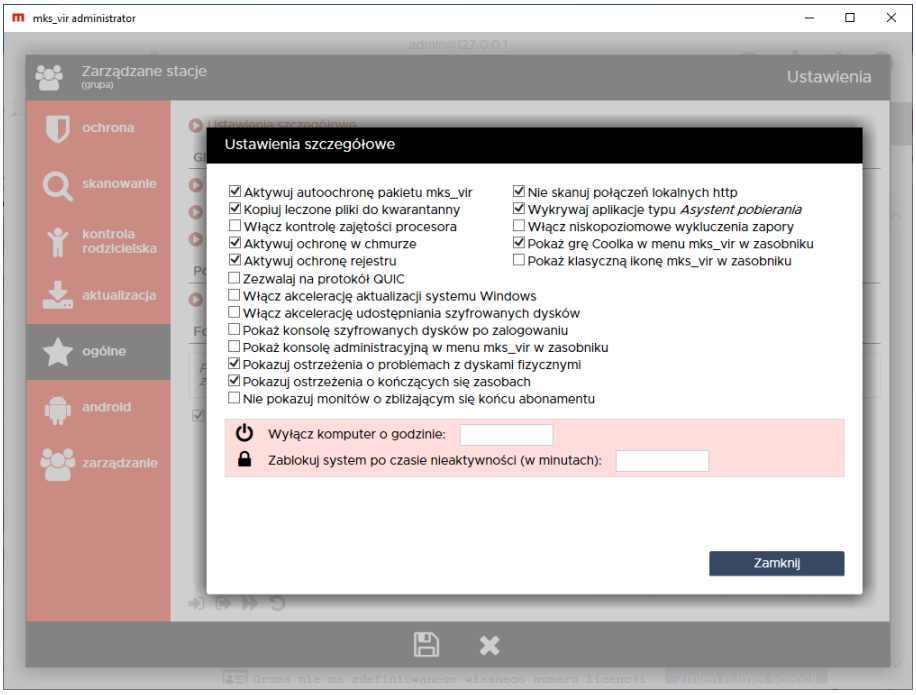
- **Potwierdzaj aktualizację modułów programu** – włączenie tej opcji powoduje, że na stacjach w przypadku konieczności aktualizacji modułów programowych (a więc innych niż bazy antywirusowe i silniki skanujące) pojawi się pytanie, czy tego dokonać; w niektórych przypadkach samoczynna aktualizacja takich elementów programu może chwilowo zaburzać działanie innych programów

Proxy – umożliwia automatyczne wykorzystanie serwerów proxy, jeśli te są dostępne

Ogólne:



Ustawienia szczegółowe – umożliwiają dostrojenie niektórych elementów programu **mks_vir** i ustalenie o której godzinie stacje powinny zostać wyłączone:



- **Aktywuj autoochronę pakietu mks_vir** – włącza mechanizmy chroniące spójność instalacji programu **mks_vir**
- **Kopiuj leczone pliki do kwarantanny** – tworzy w kwaranatannie programu **mks_vir** kopie plików leczonych lub kasowanych; funkcja pomocna w przypadku, gdyby była konieczność przywrócenia orginalnych plików (sprzed leczenia) lub wysłania ich do ponownej analizy do działu analiz **mks_vir**

- **Włącz kontrolę zajętości procesora** – włącza mechanizm zmniejszający wykorzystanie mocy obliczeniowej procesora przez mechanizmy ochronne programu **mks_vir** na mało wydajnych maszynach
- **Aktywuj ochronę w chmurze** – włącza mechanizmy ochronne programu **mks_vir** korzystające z możliwości chmury obliczeniowej **mks_vir**; do działania wymagany jest stały dostęp do internetu
- **Aktywuj ochronę rejestru** – włącza mechanizmy programu **mks_vir** chroniące zawartość i spójność rejestru systemowego
- **Zezwalaj na protokół QUIC** – wyłącza blokadę protokołu QUIC (HTTP/3):

  https://pl.wikipedia.org/wiki/HTTP/3

- **Nie skanuj połączeń lokalnych http** – wyłącza skanowanie protokołu HTTP dla połączeń realizowanych wewnątrz systemu operacyjnego (dla połączeń w adresacji 127.x.x.x)
- **Wykrywaj aplikacje typu *Asystent pobierania*** – włącza wykrywanie tzw. *Asystentów pobierania* jako zagrożeń
- **Pokaż konsolę szyfrowanych dysków po zalogowaniu** – włącza automatyczne wyświetlanie konsoli zarządzającej szyfrowanymi dyskami w programie **mks_vir** po zalogowaniu użytkownika w systemie
- **Włącz akcelerację udostępniania szyfrowanych dysków** – przyspiesza podłączanie szyfrowanych dysków do systemowych mechanizmów obsługi systemów plików
- **Pokaż konsolę administracyjną w menu mks_vir w zasobniku** – włącza dostęp do konsoli administracyjnej programu **mks_vir administrator** w menu podręcznym ikony **mks_vir** w zasobniku systemowym
- **Włącz niskopoziomowe wykluczenia zapory** – włącza obsługę wykluczeń plików lub folderów zdefiniowanych w sekcji *Lista wykluczonych plików i folderów*, w zaporze programu **mks_vir**
- **Włącz akcelerację aktualizacji systemu Windows** – automatyzuje i przyspiesza instalację nowych aktualizacji systemu Windows
- **Pokazuj ostrzeżenia o problemach z dyskami fizycznymi** – włącza powiadomienia informujące o problemach w działaniu dysków fizycznych w przypadku, gdy takie problemy są raportowane w systemie
- **Pokazuj ostrzeżenia o kończących się zasobach** – włącza powiadomienia informujące o zbyt małych zasobach dostępnych dla systemu, np. w przypadku kończącego się miejsca na dysku
- **Nie pokazuj monitów o zbliżającym się końcu abonamentu** – wyłącza powiadomienia informujące o zbliżającym się zakończeniu ważności licencji na użytkowanie programu **mks_vir**; powiadomienia o zakończonej ważności licencji będą wyświetlane
- **Pokaż grę *Coolka* w menu mks_vir w zasobniku** – włącza dostępność gry *Coolka* w menu **mks_vir** w zasobniku systemowym
- **Pokaż klasyczną ikonę mks_vir w zasobniku** – zmienia wygląd ikony programu **mks_vir** w zasobniku systemowym na „klasyczną”, znaną ze starszych wersji programu **mks_vir**

- **Wyłącz komputer o godzinie** – pozwala na zdefiniowanie godziny, o której komputer zostanie automatycznie wyłączony
- **Zablokuj system po czasie nieaktywności (w minutach)** – pozwala na zdefiniowanie po jakim czasie braku aktywności użytkownika system ma zostać zablokowany

Globalne wykluczenia ochrony – umożliwia zdefiniowanie obiektów, dla których nie będzie działała żadna ochrona, korzystanie z tych ustawień wymaga dużej rozwagi:

- **Lista wykluczonych domen internetowych** – umożliwia zdefiniowanie adresów, dla których nie będą działały moduły ochrony przeglądarki i kontroli rodzicielskiej programu **mks_vir**
- **Lista wykluczonych plików i folderów** – umożliwia zdefiniowanie obiektów (plików lub folderów), dla których nie będzie działał moduł ochrony plików programu **mks_vir**
- **Lista wykluczonych procesów** – umożliwia zdefiniowanie procesów (programów), dla których nie będzie działał moduł ochrony plików programu **mks_vir**

Porty i protokoły – umożliwia zdefiniowane dla których portów mają działać moduły ochrony poczty, ochrony przeglądarki i kontroli rodzicielskiej oraz jakie porty mają być w ogóle wyłączone spod kontroli, również w zaporze programu **mks_vir**; definiuje się je w **Tabeli skanowanych i wykluczonych portów i protokołów**

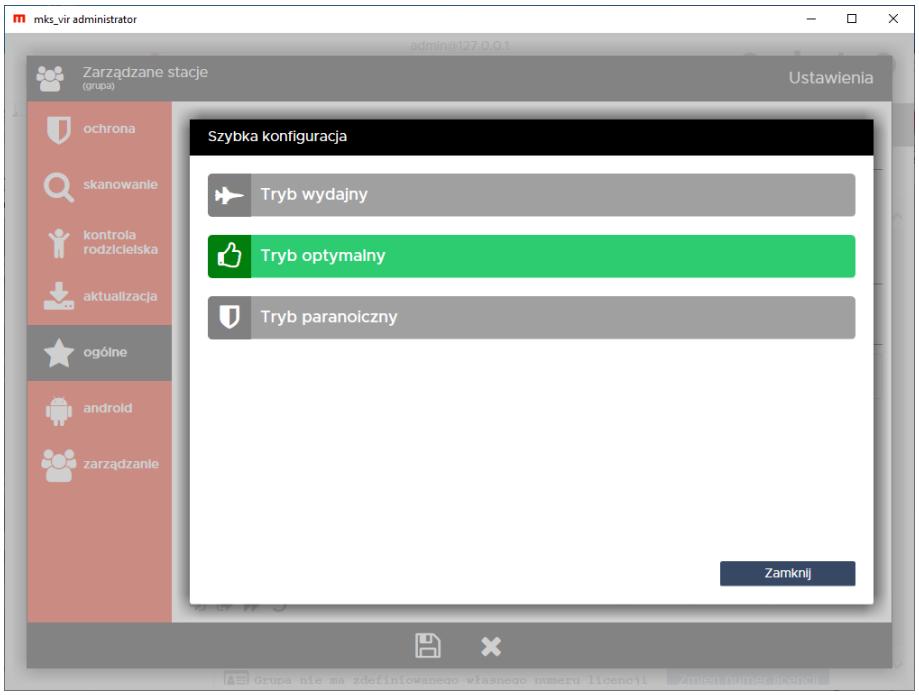
Folder danych – umożliwia określenie innego niż domyślny folderu dla dużych ilości danych (kwarantanna, *SafeStorage*, kopie zapasowe, szyfrowane dyski); zdefiniowanie innego niż domyślny folderu wymaga, by dysk twardy na którym ma się znajdować, był dostępny w komputerze

– pozwala na odtworzenie wcześniej wyeksportowanych ustawień programu **mks_vir** *(importuj ustawienia)*

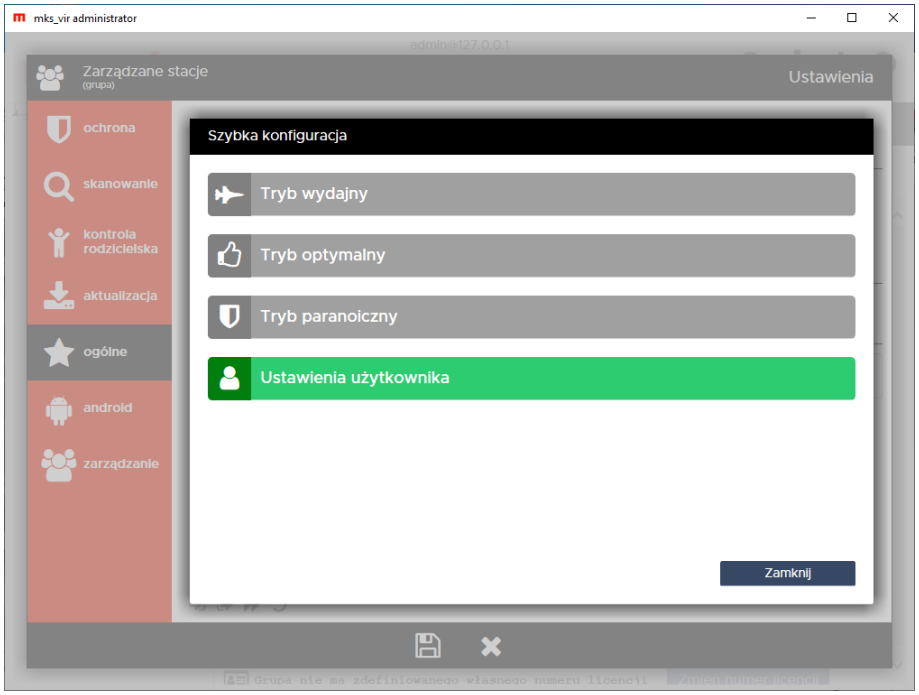
– pozwala na wyeksportowanie aktualnych ustawień programu **mks_vir** *(eksportuj ustawienia)*

– pozwala na wybór predefiniowanych profili konfiguracyjnych programu **mks_vir** *(szybka konfiguracja):*

- **Tryb wydajny** – zestaw ustawień zapewniający wysoką wydajność pracy nawet na słabszych maszynach
- **Tryb optymalny** – optymalny zestaw ustawień ochrony proponowany przez producenta
- **Tryb paranoiczny** – zestaw ustawień gwarantujący ekstremalnie wysoki poziom ochrony. Ten zestaw ustawień może powodować zauważalne spowalnianie pracy systemu

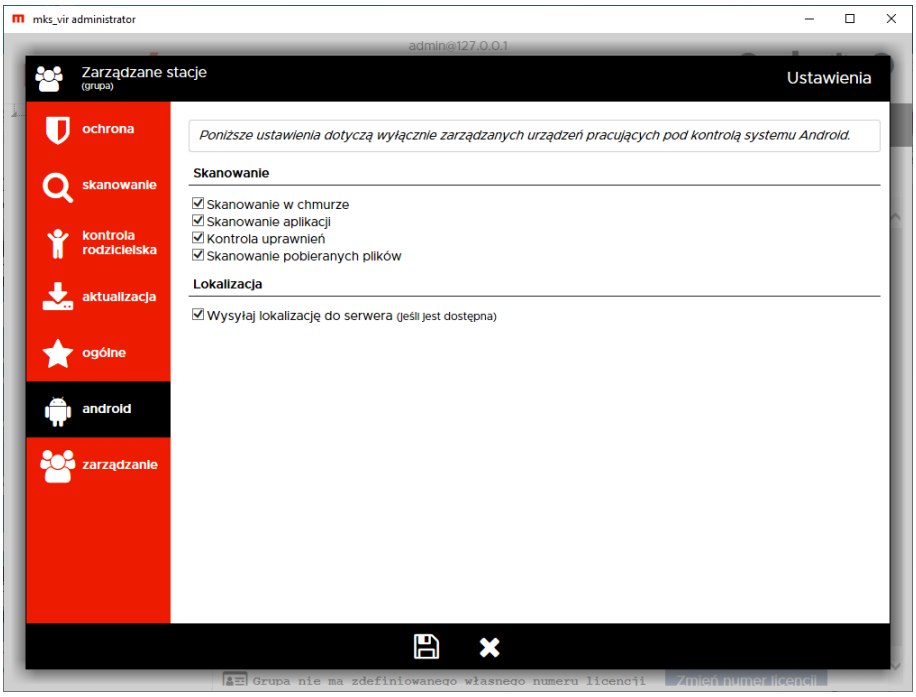


- **Ustawienia użytkownika** – informacja pojawiająca się w przypadku, gdy aktualna konfiguracja programu **mks_vir** nie odpowiada żadnemu z predefiniowanych profili



↺ – przywraca domyślną konfigurację programu **mks_vir** *(przywróć ustawienia domyślne)*

Android:



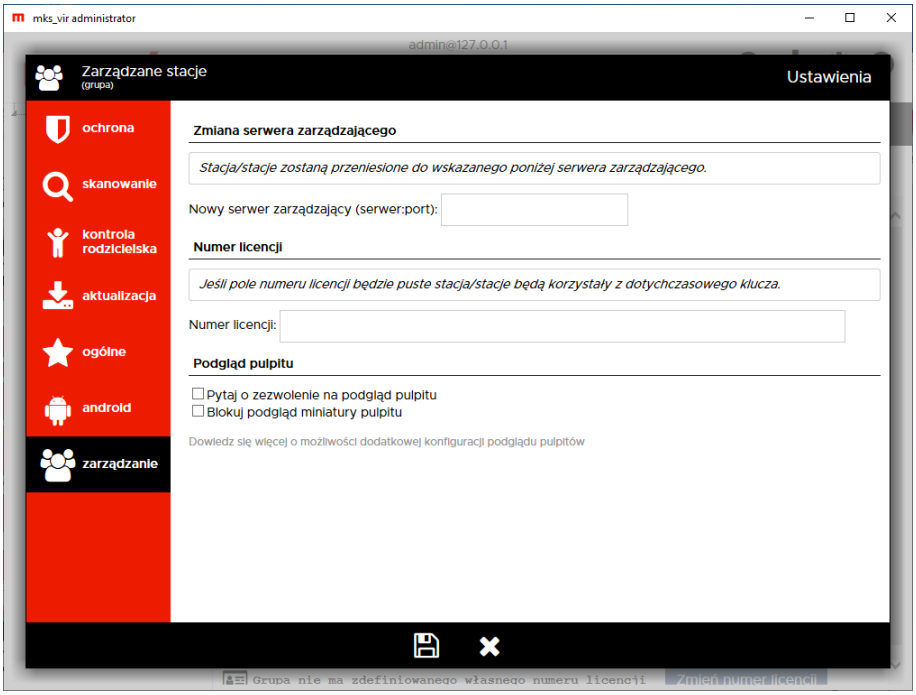
Skanowanie:

- **Skanowanie w chmurze** – umożliwia weryfikację skanowanych obiektów w chmurze obliczeniowej **mks_vir** i zależnie od wyniku określanie, czy dany obiekt jest zdrowy, czy nie (przesyłane są w takich przypadkach tylko sygnatury skanowanych obiektów; w przypadku braku sygnatury w bazie chmury obliczeniowej, przesyłany jest cały obiekt do dalszej analizy)
- **Skanowanie aplikacji** – skanuje zainstalowane aplikacje w poszukiwaniu aplikacji szkodliwych
- **Kontrola uprawnień** – sprawdza uprawnienia zainstalowanych aplikacji i w zależności od charakteru aplikacji informuje, jeśli te uprawnienia są zbyt wysokie
- **Skanowanie pobieranych plików** – pliki pobierane z internetu są automatycznie skanowane i w razie wykrycia zagrożenia usuwane

Lokalizacja:

- **Wysyłaj lokalizację do serwera** – przesyła do serwera zarządzającego lokalizację urządzenia (opartą zarówno na triangulacji względem stacji przekaźnikowych, jak i na GPS – zależnie od tego, która z metod jest dostępna), co pozwala na śledzenie położenia danego urządzenia

Zarządzanie:



Zmiana serwera zarządzającego – umożliwia szybkie przełączenie stacji lub grupy stacji z jednego serwera zarządzającego **mks_vir administrator**, do drugiego

Numer licencji – umożliwia szybką aktualizację/zmianę licencji na stacjach

Podgląd pulpitu – umożliwia określenie, czy w pulpit stacji ma być widoczny w podglądach stacji w konsoli zarządzającej

- **Pytaj o zezwolenie na podgląd pulpitu** – umożliwia określenie, czy w przypadku wybrania podglądu pulpitu dla stacji użytkownik ma być pytany o zgodę, czy nie
- **Blokuj podgląd miniatury pulpitu** – umożliwia określenie, czy w przypadku wybrania podglądu pulpitów w grupie, podgląd ma być dostępny, czy nie