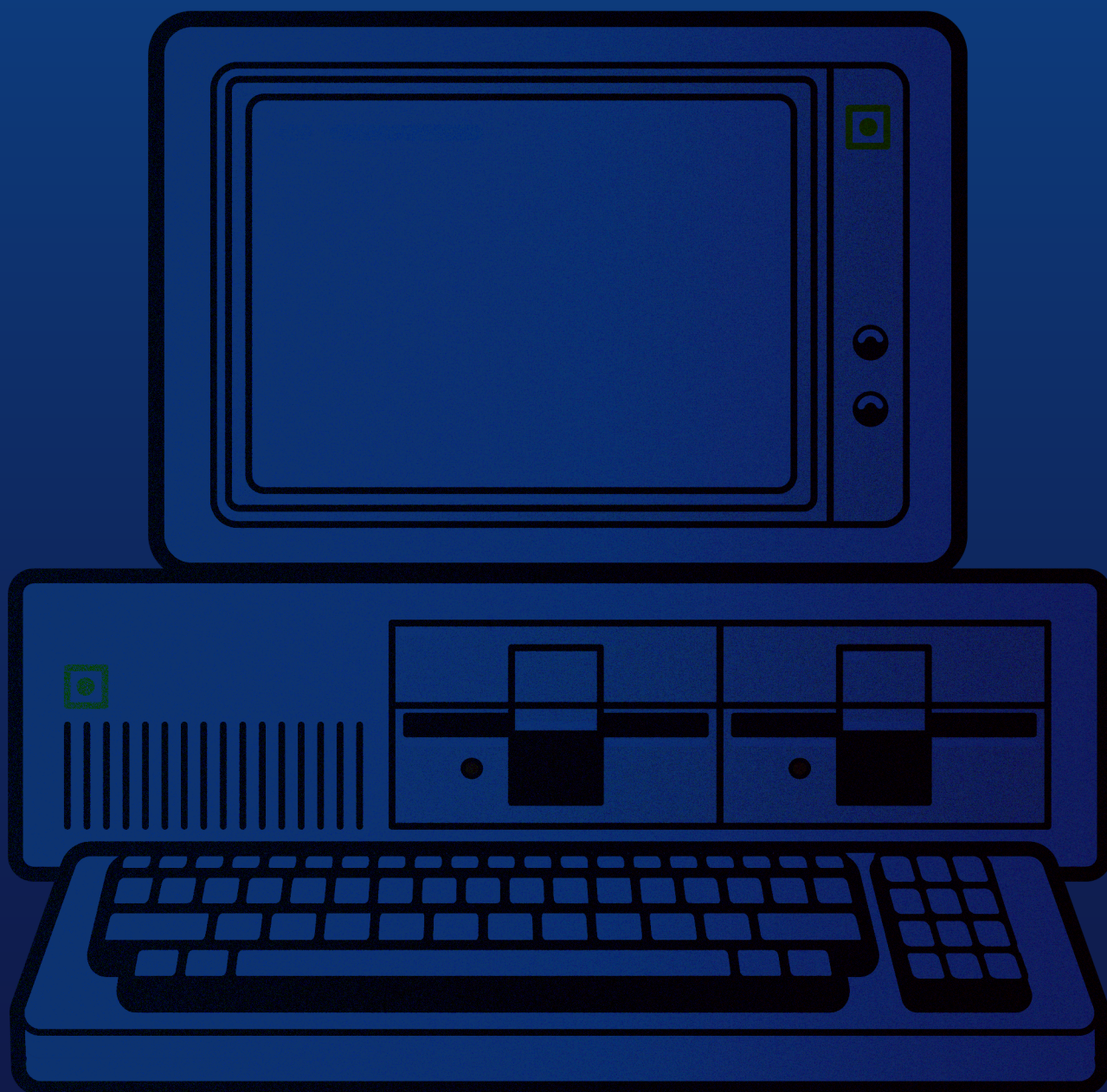


mks_vir

Podręcznik



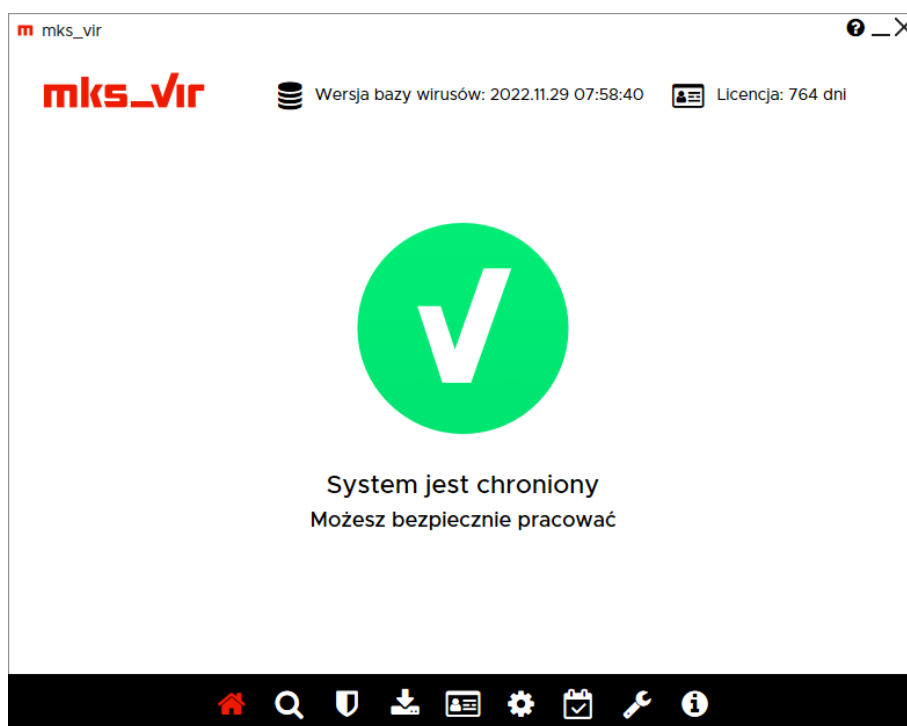
mks_vir	2
• Skanowanie	3
• Ochrona	4
• Aktualizacja	5
• Licencja	5
• Ustawienia	6
• Raporty	6
• Narzędzia	8
• Informacje	11
Szczegółowe ustawienia pakietu	12
Ochrona → Ochrona plików	12
Ochrona → SafeStorage	13
Ochrona → Ochrona poczty	15
Ochrona → Ochrona przeglądarki	16
Ochrona → Zapora sieciowa (firewall)	17
Ochrona → Kontrola urządzeń USB	18
Ochrona → Kontrola urządzeń multimedialnych	20
Ochrona → Kontrola aplikacji	21
Ochrona → Ochrona RoundKick EDR	22
Ochrona → Bezpieczna przeglądarka	25
Skanowanie → Skanowanie pełne	26
Skanowanie → Skanowanie szybkie	27
Skanowanie → Kwarantanna	28
Kontrola rodzicielska	29
Aktualizacja	31
Ogólne	32
Aktualizacja programu w sieciach lokalnych za pomocą mechanizmu repozytorium udostępnianego po HTTP	36
Aktualizacja programu na stacjach bez dostępu do sieci za pomocą mechanizmu repozytorium	38
Sygnalizacja wykrycia zagrożenia przez moduł „Ochrona plików”	40
Sygnalizacja próby połączenia przez moduł „Zapory”	41


Sygnalizacja podłączenia urządzenia USB przez moduł „Kontroli urządzeń USB” . . .	42
Sygnalizacja dostępu aplikacji do urządzenia multimedialnego przez moduł „Kontroli urządzeń multimedialnych”	43
Jak odblokować aplikację zablokowaną w „Zaporze”	44
Jak zmodyfikować regułę w module „Kontrola urządzeń USB”	47
Jak zmodyfikować regułę w module „Kontrola urządzeń multimedialnych”	50
Jak utworzyć regułę w module „Kontrola aplikacji”	52
Jak utworzyć i zmodyfikować reguły użytkownika w module „Kontrola rodzicielska” .	56
Jak dodać domenę internetową do wykluczeń	60
Jak dodać plik lub folder do wykluczeń	62
Jak dodać proces do wykluczeń	64
Jak dodać porty do wykluczeń	66
Jak utworzyć i wysłać audyt systemu	68
Jak utworzyć nośnik ratunkowy „Rescue Disk”	70
Korzystanie z nośnika ratunkowego „Rescue Disk”	71
Zarządzanie szyfrowanymi dyskami	77
Korzystanie z menadżera haseł	82
Korzystanie ze skanera command line	90
Korzystanie z bezpiecznej przeglądarki	93
Korzystanie z kopii zapasowych (backup)	98
Odzyskiwanie danych za pomocą SafeStorage	104
Korzystanie z modułu czyszczenia systemu	107
Skanowanie programem mks_vir w trybie awaryjnym Windows	111
mks_vir administrator	115
• Podstawowe informacje o grupie	117
• Podstawowe informacje o stacji	120
• Ustawienia	124
• Raporty	125
• Oprogramowanie	128
• Podsumowanie	128
Szczegółowe ustawienia pakietu	130
Ochrona → Ochrona plików	130
Ochrona → SafeStorage	131
Ochrona → Ochrona poczty	133
Ochrona → Ochrona przeglądarki	134
Ochrona → Zapora sieciowa (firewall)	135
Ochrona → Kontrola urządzeń USB	136

Ochrona → Kontrola urządzeń multimedialnych	138
Ochrona → Kontrola aplikacji	139
Ochrona → Ochrona RoundKick EDR	140
Ochrona → Bezpieczna przeglądarka	142
Skanowanie → Skanowanie pełne	143
Skanowanie → Skanowanie szybkie	144
Skanowanie → Kwarantanna	145
Kontrola rodzicielska	145
Aktualizacja	147
Ogólne	148
Android	152
Zarządzanie	153
Dodawanie reguł w module „Kontrola urządzeń USB”	154
Tworzenie i modyfikacja reguł użytkownika w module „Kontrola rodzicielska”	156
Jak utworzyć i wysłać audyt systemu z konsoli	159
Zarządzanie uprawnieniami	162
Zarządzanie bazą	166
Ustawianie powiadomień email	168
Ustawianie powiadomień syslog	171
Jak przeinstalować program mks_vir administrator z zachowaniem ustawień	174
Jak przenieść program mks_vir administrator na inny komputer w sieci z zachowaniem ustawień	176
Zalety korzystania z programu mks_vir administrator w sieciach lokalnych (LAN)	179
Instalacja	182
Instalacja programu mks_vir	182
Instalacja programu mks_vir administrator	187
Instalacja programu mks_vir endpoint	191
Automatyczna instalacja programu mks_vir	195
Automatyczna instalacja programu mks_vir w trybie niezarządzanym	195
Automatyczna instalacja programu mks_vir w trybie zarządzanym	195
Automatyczna instalacja programu mks_vir w trybie zarządzanym w domenie Windows	196
mks_vir dla systemu Android	197
Wymagania systemowe programów mks_vir	201
Umowa licencyjna	202

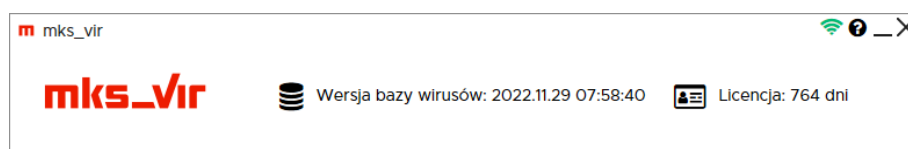
mks_vir

Ekran startowy programu **mks_vir** oraz podstawowe informacje o stanie ochrony:

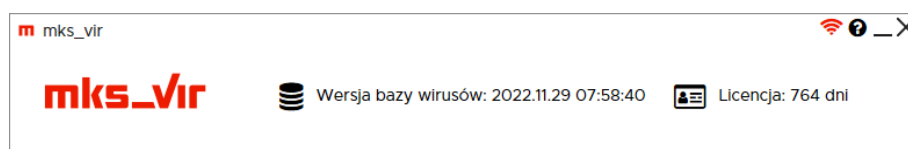


W przypadku programu **mks_vir** zarządzanego za pomocą programu **mks_vir administrator** w prawym górnym narożniku okna widoczna jest ikona  sygnalizująca aktualną dostępność serwera zarządzającego **mks_vir administrator**:

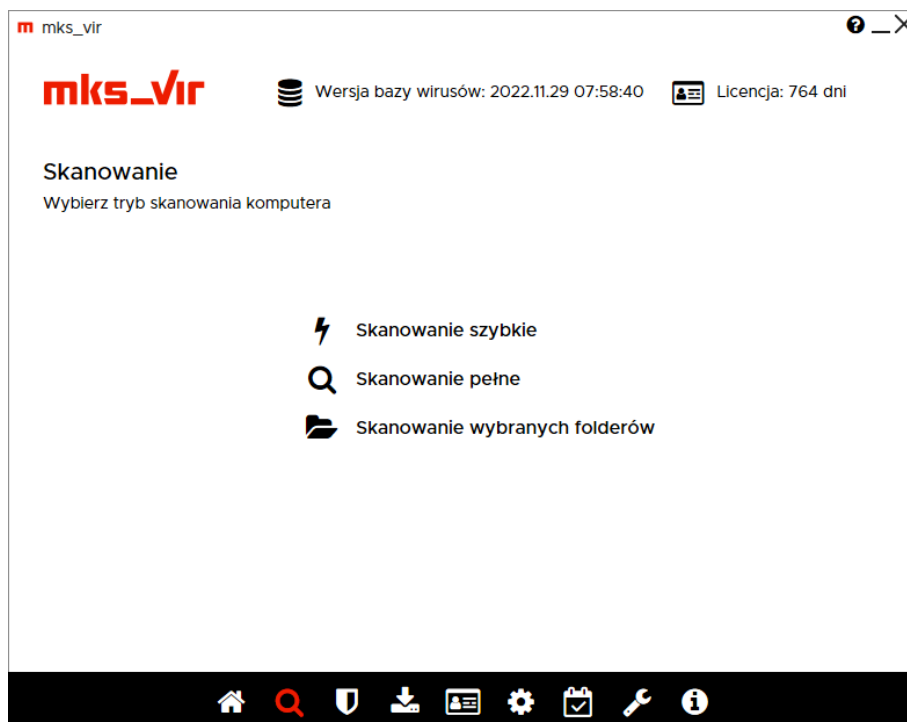
 – serwer zarządzający **mks_vir administrator** jest dostępny:



 – serwer zarządzający **mks_vir administrator** jest niedostępny:



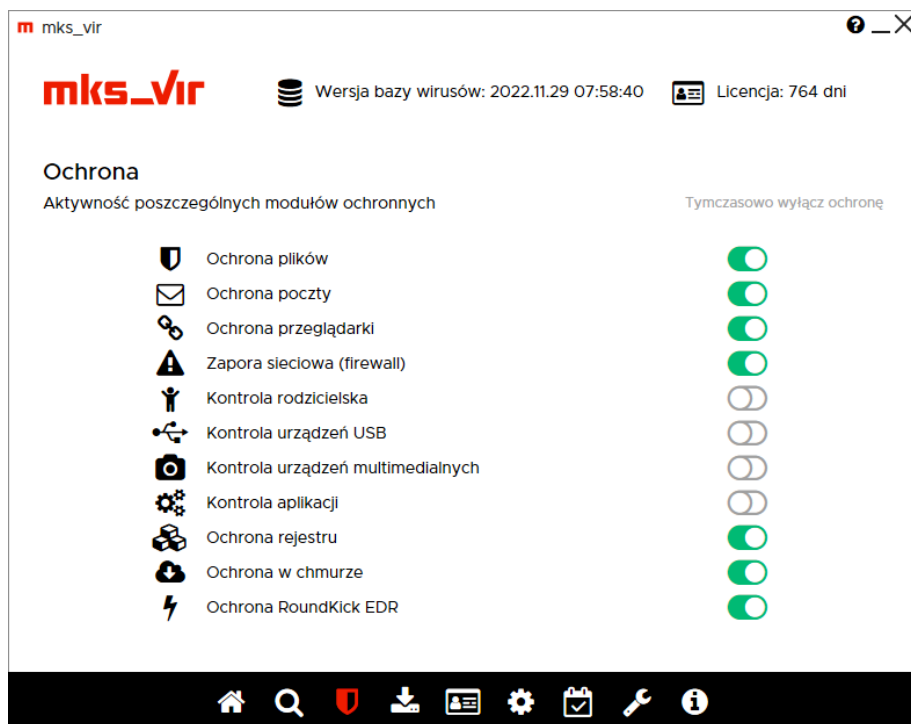
Skanowanie:



Umożliwia wybranie trybu skanowania:

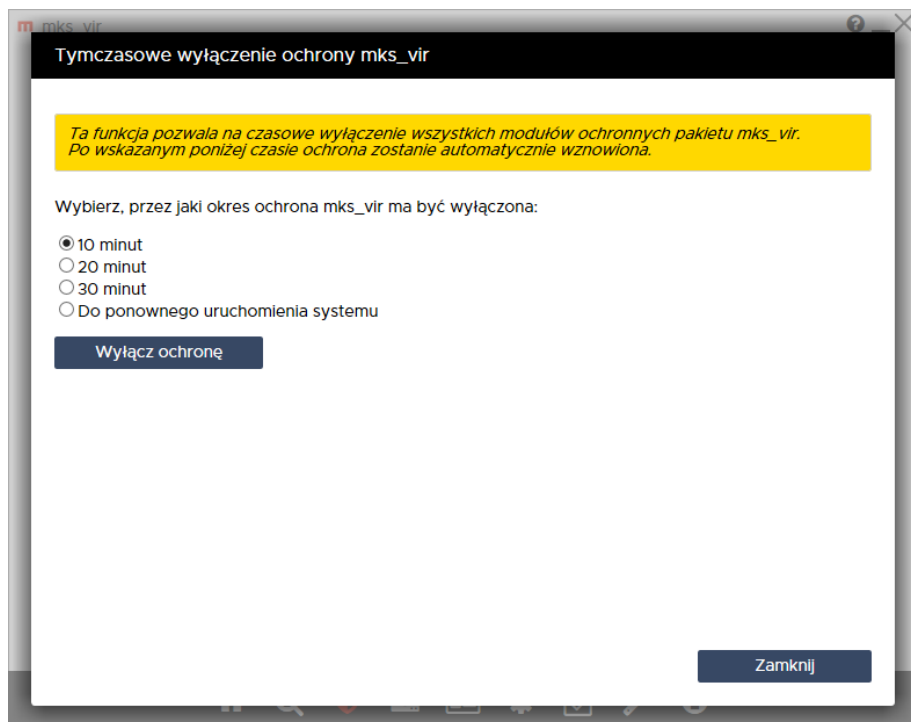
- **Skanowanie szybkie** – umożliwia przeskanowanie pamięci systemu oraz załadowanych i uruchomionych serwisów, procesów i innych obiektów (biblioteki, drivery itp.)
- **Skanowanie pełne** – umożliwia przeskanowanie zawartości wszystkich dostępnych dysków
- **Skanowanie wybranych folderów** – umożliwia przeskanowanie zawartości wybranych folderów

Ochrona:

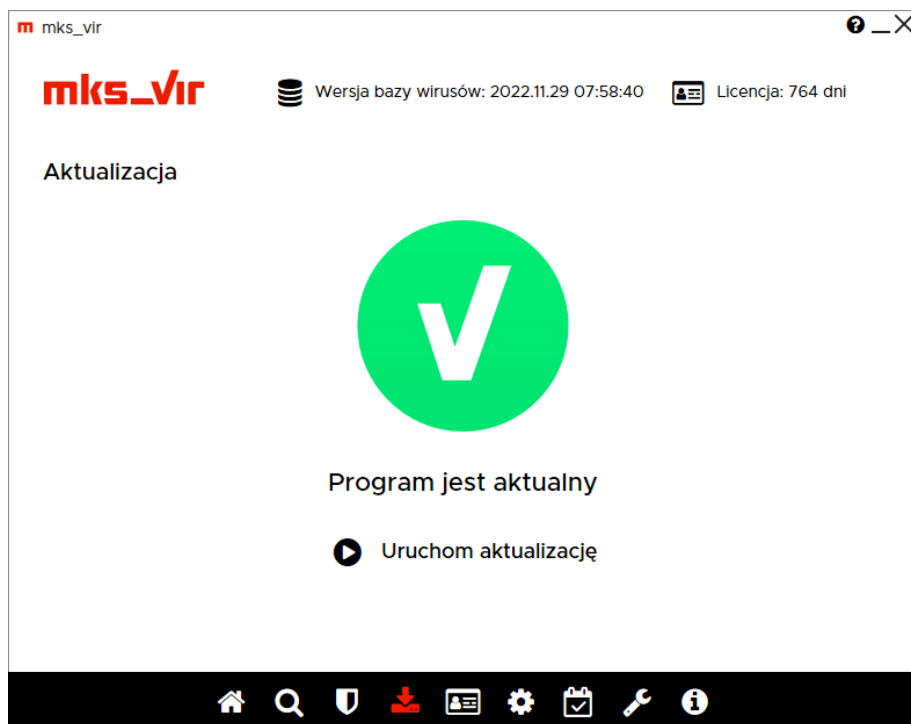


Pokazuje aktualny stan poszczególnych modułów ochronnych programu **mks_vir** umożliwiając jednocześnie ich szybkie wyłączenie lub włączenie.

- **Tymczasowo wyłącz ochronę** – umożliwia szybkie wyłączenie wszystkich modułów ochronnych (gdy zachodzi taka potrzeba):

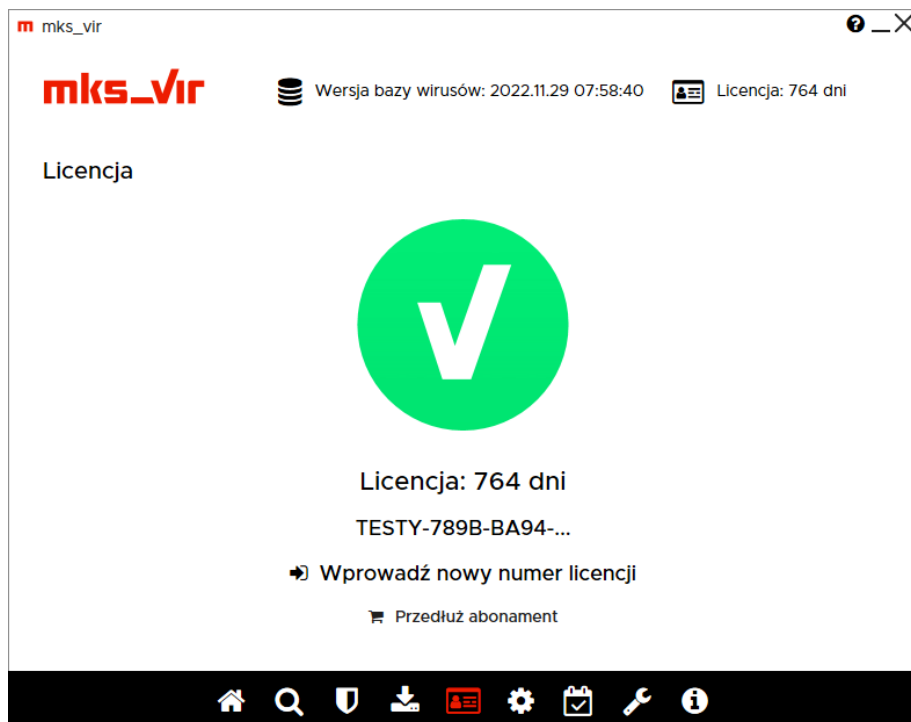


Aktualizacja:



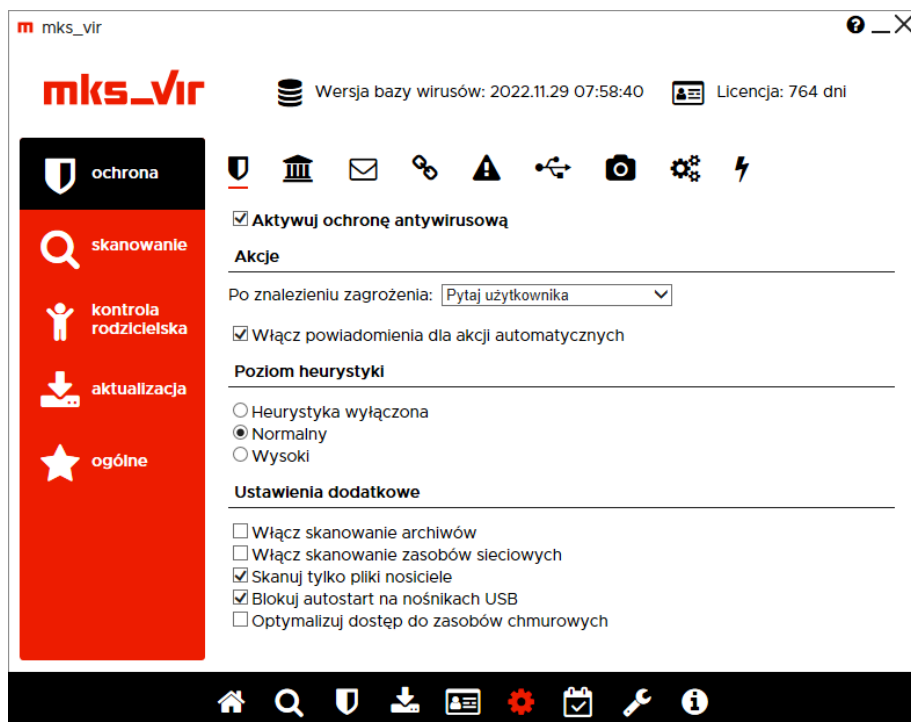
Pokazuje aktualny stan aktualizacji programu **mks_vir** oraz pozwala uruchomić jego aktualizację.

Licencja:



Podaje aktualny stan licencji programu **mks_vir**, wyświetla jego początkowy fragment oraz umożliwia wprowadzenie nowego (w przypadku gdy wymagana jest zmiana tej licencji lub wprowadzenie nowej w przypadku wygaśnięcia starej).

Ustawienia:



Pozwala na dostęp do szczegółowych ustawień programu **mks_vir**.
 „Szczegółowe ustawienia pakietu **mks_vir**”

Raporty:

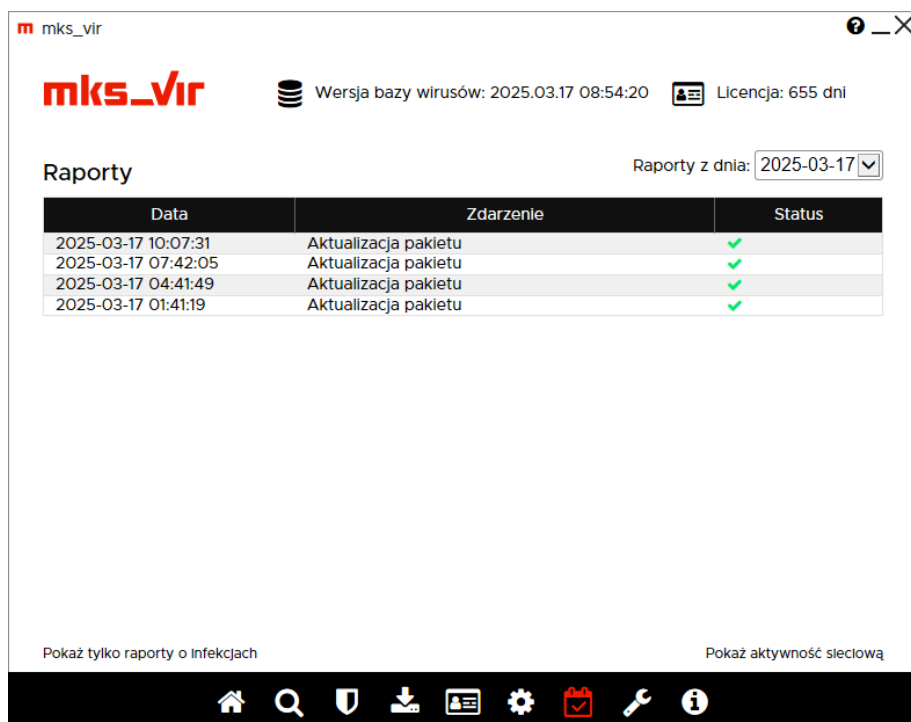
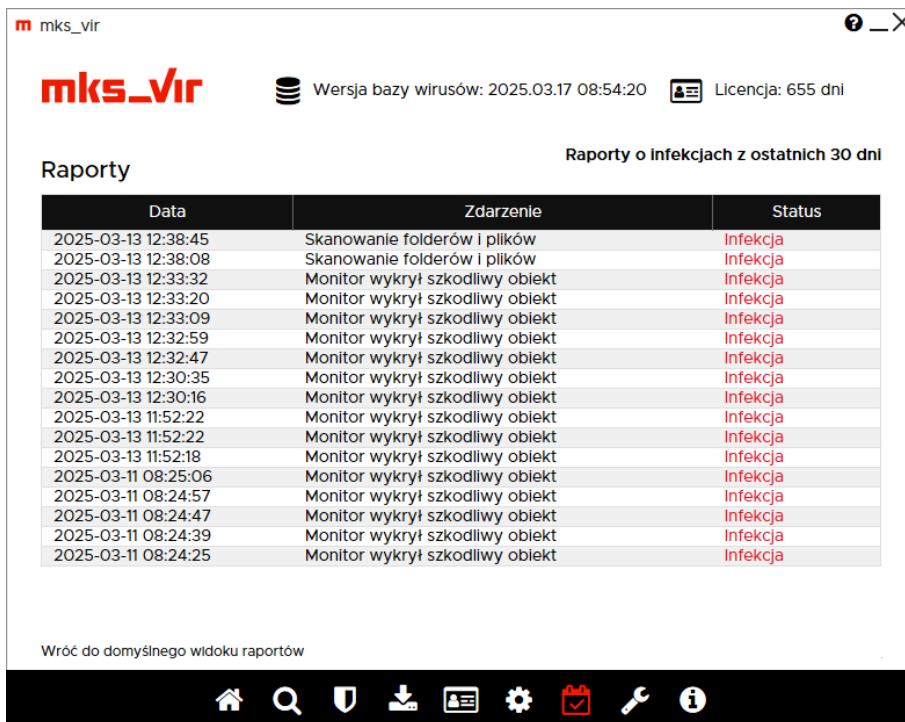


Tabela z widocznymi w niej poszczególnymi raportami aktywności programu **mks_vir** (aktualizacje, wykryte infekcje, skanowania itp.).

Po wybraniu „Pokaż tylko raporty o infekcjach” pojawią się tylko raporty z wykrytymi infekcjami w ostatnich 30 dniach; powrót do normalnego wyświetlania raportów jest możliwy przez wybranie „Wróć do domyślnego widoku raportów”:

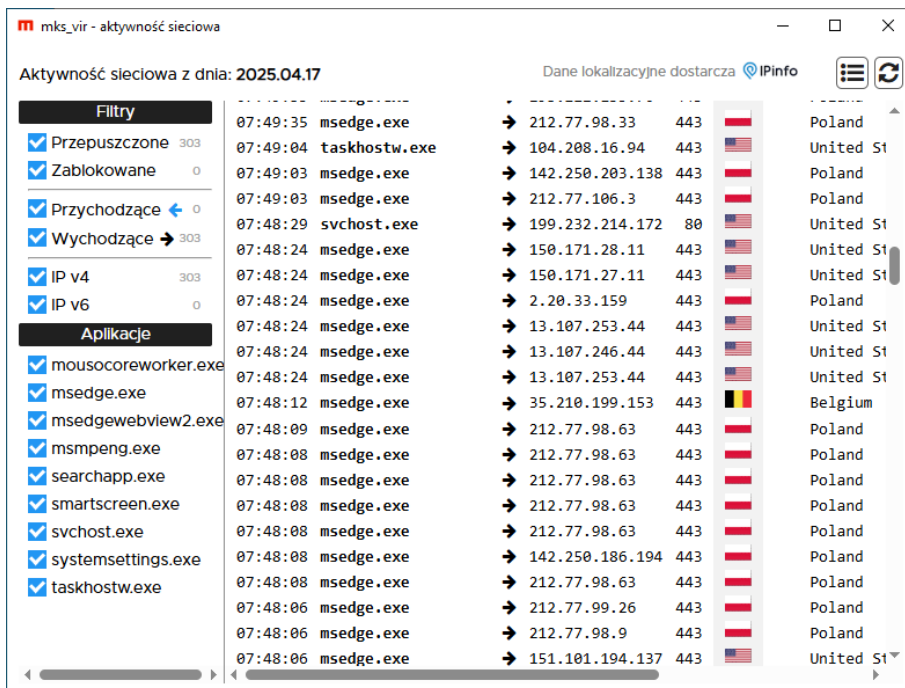


Raporty o infekcjach z ostatnich 30 dni

Data	Zdarzenie	Status
2025-03-13 12:38:45	Skanowanie folderów i plików	Infekcja
2025-03-13 12:38:08	Skanowanie folderów i plików	Infekcja
2025-03-13 12:33:32	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:33:20	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:33:09	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:32:59	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:32:47	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:30:35	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:30:16	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:22	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:22	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:18	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:25:06	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:57	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:47	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:39	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:25	Monitor wykrył szkodliwy obiekt	Infekcja

Wróć do domyślnego widoku raportów

Po wybraniu „Pokaż aktywność sieciową” pojawi się okno pozwalające na przeglądanie aktywności sieciowej systemu i zainstalowanych aplikacji:



Aktywność sieciowa z dnia: 2025.04.17

Dane lokalizacyjne dostarcza IPInfo

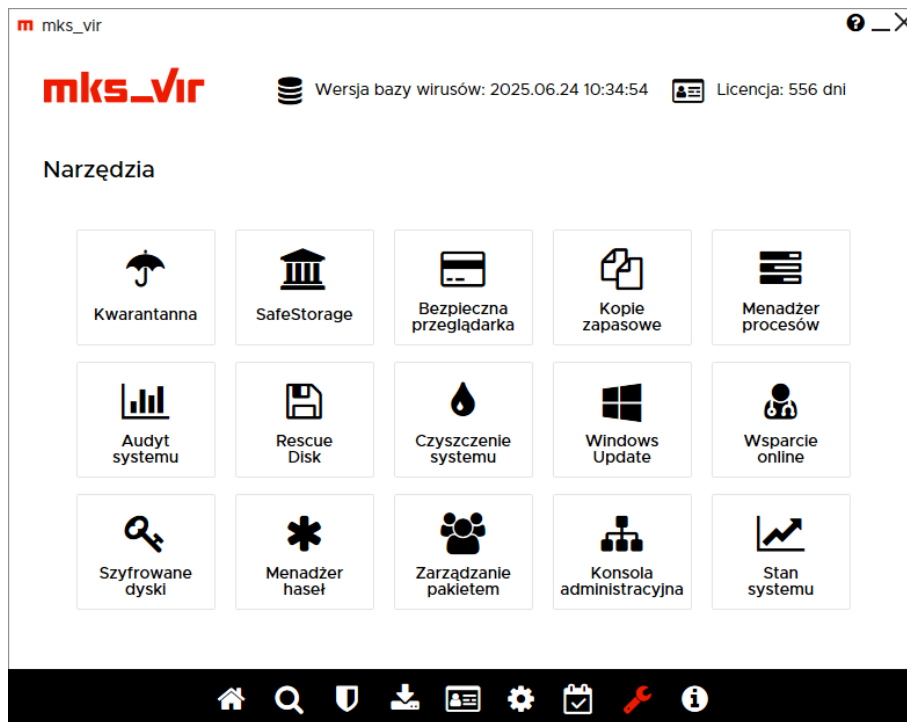
Filtry	Time	Application	IP	Port	Country
<input checked="" type="checkbox"/> Przepuszczone 303	07:49:35	msedge.exe	212.77.98.33	443	Poland
<input checked="" type="checkbox"/> Zablokowane 0	07:49:04	taskhostw.exe	104.208.16.94	443	United St
<input checked="" type="checkbox"/> Przychodzące 0	07:49:03	msedge.exe	142.250.203.138	443	Poland
<input checked="" type="checkbox"/> Wychodzące 303	07:49:03	msedge.exe	212.77.106.3	443	Poland
<input checked="" type="checkbox"/> IP v4 303	07:48:29	svchost.exe	199.232.214.172	80	United St
<input checked="" type="checkbox"/> IP v6 0	07:48:24	msedge.exe	150.171.28.11	443	United St
<input checked="" type="checkbox"/> Aplikacje	07:48:24	msedge.exe	150.171.27.11	443	United St
<input checked="" type="checkbox"/> mousocoreworker.exe	07:48:24	msedge.exe	2.20.33.159	443	Poland
<input checked="" type="checkbox"/> msedge.exe	07:48:24	msedge.exe	13.107.253.44	443	United St
<input checked="" type="checkbox"/> msedgewebview2.exe	07:48:24	msedge.exe	13.107.246.44	443	United St
<input checked="" type="checkbox"/> msmtpeng.exe	07:48:24	msedge.exe	13.107.253.44	443	United St
<input checked="" type="checkbox"/> searchapp.exe	07:48:12	msedge.exe	35.210.199.153	443	Belgium
<input checked="" type="checkbox"/> smartscreen.exe	07:48:09	msedge.exe	212.77.98.63	443	Poland
<input checked="" type="checkbox"/> svchost.exe	07:48:08	msedge.exe	212.77.98.63	443	Poland
<input checked="" type="checkbox"/> systemsettings.exe	07:48:08	msedge.exe	212.77.98.63	443	Poland
<input checked="" type="checkbox"/> taskhostw.exe	07:48:08	msedge.exe	212.77.98.63	443	Poland
	07:48:08	msedge.exe	212.77.98.63	443	Poland
	07:48:08	msedge.exe	212.77.98.63	443	Poland
	07:48:08	msedge.exe	212.77.98.63	443	Poland
	07:48:08	msedge.exe	212.77.98.63	443	Poland
	07:48:06	msedge.exe	212.77.99.26	443	Poland
	07:48:06	msedge.exe	212.77.98.9	443	Poland
	07:48:06	msedge.exe	151.101.194.137	443	United St

- **Filtry** – pozwala na filtrację aktywności:
 - dla połączeń przepuszczonych lub **zablokowanych**
 - dla połączeń przychodzących (←) lub wychodzących (→)

– dla połączeń na protokołach **IP v4** lub **IP v6**

- **Aplikacje** – pozwala na filtrację aktywności połączeń dla określonych aplikacji

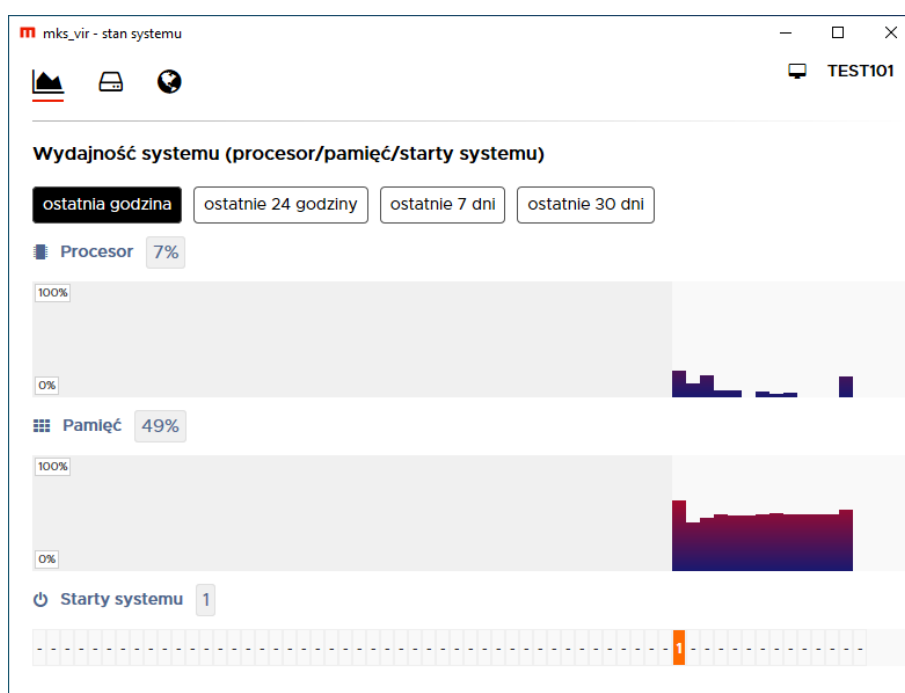
Narzędzia:



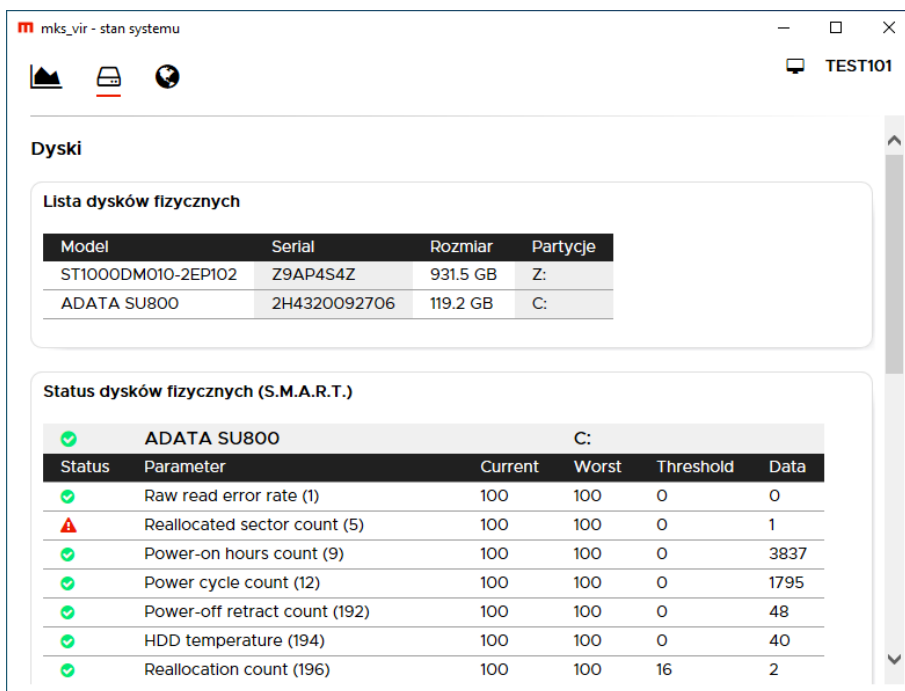
Dostęp do dodatkowych narzędzi programu **mks_vir**:

- **Kwarantanna** – zarządzanie zawartością folderu kwarantanny
- **SafeStorage** – zarządzanie zawartością folderu *SafeStorage*
- **Bezpieczna przeglądarka** – dostęp do bezpiecznej przeglądarki internetowej, zalecanej szczególnie w przypadku dostępu do witryn bankowych
- **Kopie zapasowe** – zarządzanie i konfiguracja kopii zapasowych (backup)
- **Menadżer procesów** – zarządzanie uruchomionymi w systemie procesami
- **Audyt systemu** – umożliwia wygenerowanie i wysłanie audytu systemu w celu jego dalszej analizy w dziale analiz **mks_vir**
- **Rescue disk** – umożliwia wygenerowanie aktualnego nośnika (CD/DVD lub USB) pozwalającego przeskanowanie zasobów komputera w pełnej izolacji od zainstalowanego systemu operacyjnego
- **Czyszczenie systemu** – umożliwia szybką analizę i usunięcie niepotrzebnych obiektów zaśmiecających dyski komputera
- **Windows Update** – umożliwia dostęp do systemowego Windows Update
- **Wsparcie online** – umożliwia dostęp do bezpośredniego wsparcia online dla klientów programu **mks_vir**

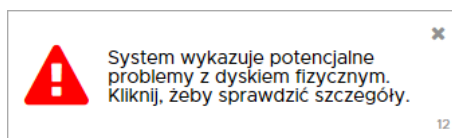
- **Szyfrowane dyski** – umożliwia tworzenie i zarządzanie dyskami szyfrowanymi programu **mks_vir**
- **Menadżer haseł** – umożliwia bezpieczne przechowywanie, korzystanie i generowanie silnych haseł do różnych usług (bankowych, portali społecznościowych itp.)
- **Zarządzanie pakietem** – opcja pozwalająca na podłączenie programu **mks_vir** do serwera zarządzającego **mks_vir administrator**
- **Konsola administracyjna** – dostęp do programu konsoli **mks_vir administrator**; pozwala na lokalne lub zdalne zarządzanie serwerami zarządzającymi **mks_vir administrator**
- **Stan systemu** – moduł pozwalający na ocenę wybranych parametrów pracy systemu:
 - Wydajność systemu:



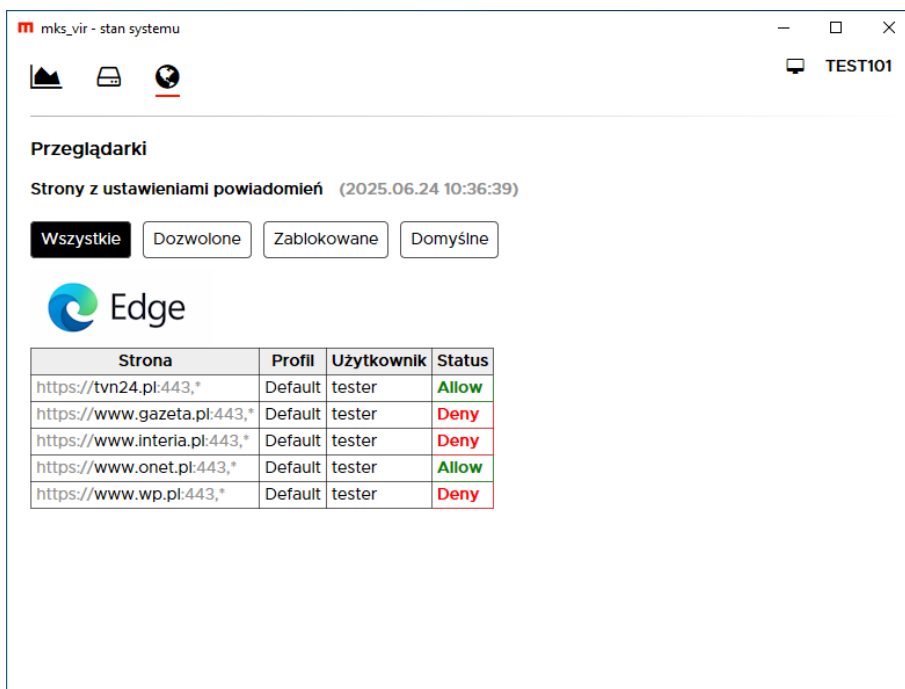
- Dyski:




Występowanie problemów w działaniu dysku twardego (jednego lub kilku, zależnie od konfiguracji komputera) będzie powodowało pojawianie się odpowiedniego komunikatu:



– Przeglądarki:



Informacje:



The screenshot displays the mks_vir application window. At the top left is the mks_vir logo. To its right, it shows 'Wersja bazy wirusów: 2022.11.29 07:58:40' and 'Licencja: 764 dni'. Below this, the interface is divided into three sections: 'Sprzęt i system', 'Pakiet mks_vir', and 'Kontakt'. The 'Sprzęt i system' section lists hardware details. The 'Pakiet mks_vir' section shows license information. The 'Kontakt' section provides the company's address and website.

Sprzęt i system

Procesor:	Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz (3600 MHz)
Pamięć:	15 GB
Grafika:	Intel(R) UHD Graphics 630
Dyski:	C: 118.5 GB 85.7 GB Z: 447 GB 405.6 GB
System:	Microsoft Windows 11 Pro (64-bitowy)

Pakiet mks_vir

Numer licencji:	TESTY-789B-BA94-...
Licencja:	764 dni
Wersja bazy:	2022.11.29 07:58:40

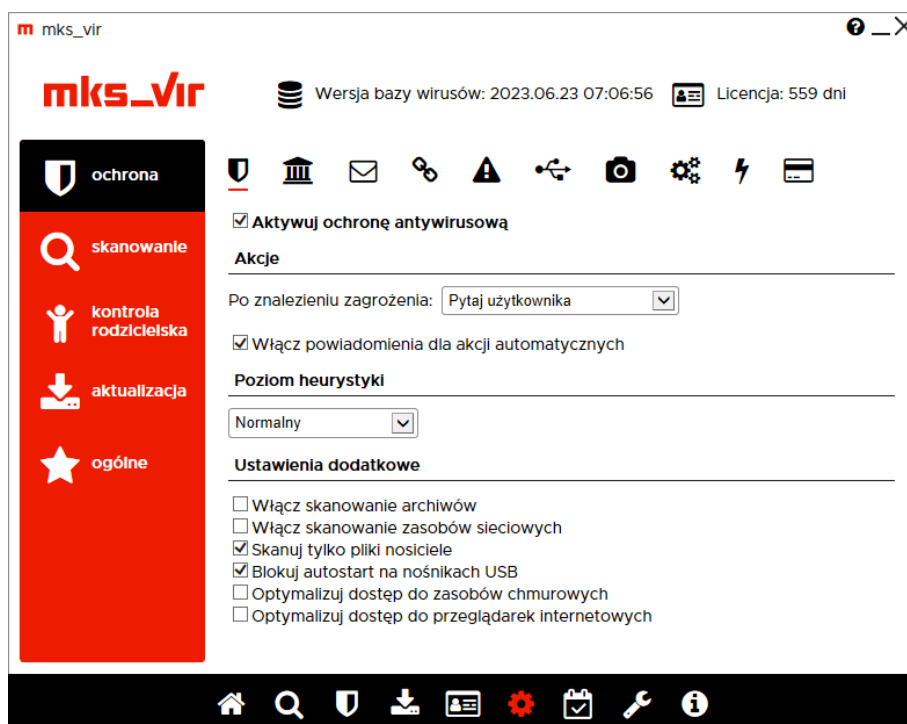
Kontakt

mks_vir Sp. z o.o.
ul. Graniczna 50
05-082 Blizne Łaszczyńskiego
(Warszawa/Bemowo)
biuro@mks-vir.pl
<http://www.mks-vir.pl>

Informacje na temat systemu, stanu licencji i aktualizacji programu **mks_vir** oraz informacje kontaktowe.

Szczegółowe ustawienia pakietu

Ochrona → Ochrona plików:



Aktywuj ochronę antywirusową – opcja aktywuje najważniejszy moduł ochronny pakietu mks_vir

Akcje – pozwala na określenie jaka akcja ma być podjęta w przypadku znalezienia zagrożenia

- **Po znalezieniu zagrożenia** – umożliwi wybranie akcji, 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
 - **Pytaj użytkownika** – blokuje zainfekowany plik i wyświetla okno, gdzie można wybrać odpowiednią akcję lub wysłać plik do działu analiz mks_vir
- **Włącz powiadomienia dla akcji automatycznych** – włącza wyświetlanie okien powiadomień modułu ochrony plików w przypadku znalezienia zagrożenia i wykonania wybranej akcji automatycznej (akcje automatyczne to „Usuń zagrożenie”, „Skasuj plik” i „Przenieś plik do kwarantanny”)

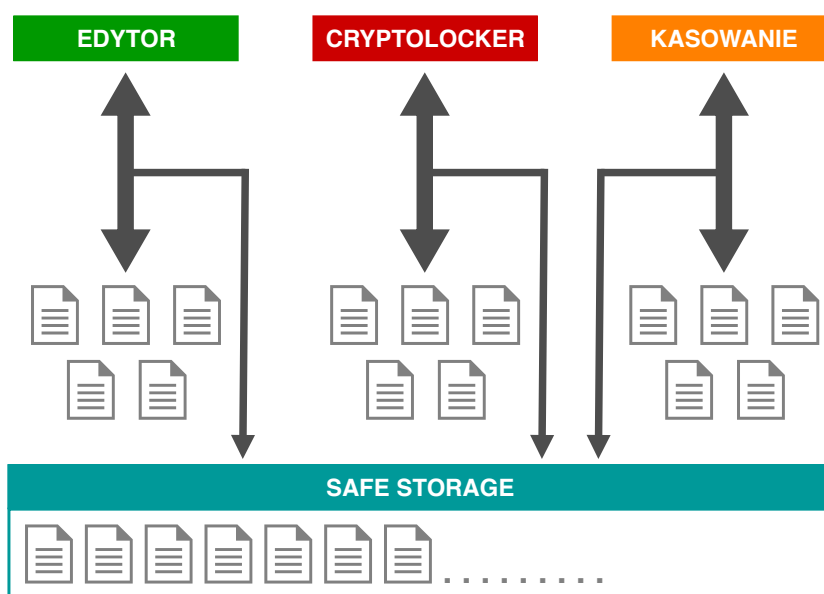
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

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 nośniki** – opcja powoduje, że sprawdzane są tylko pliki będące domyślnymi nośnikami zagrożeń, jak np. pliki EXE, COM, JS, VBS itp.
- **Blokuj autostart na nośnikach USB** – uniemożliwia automatyczne uruchomienie z podłączonych 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.



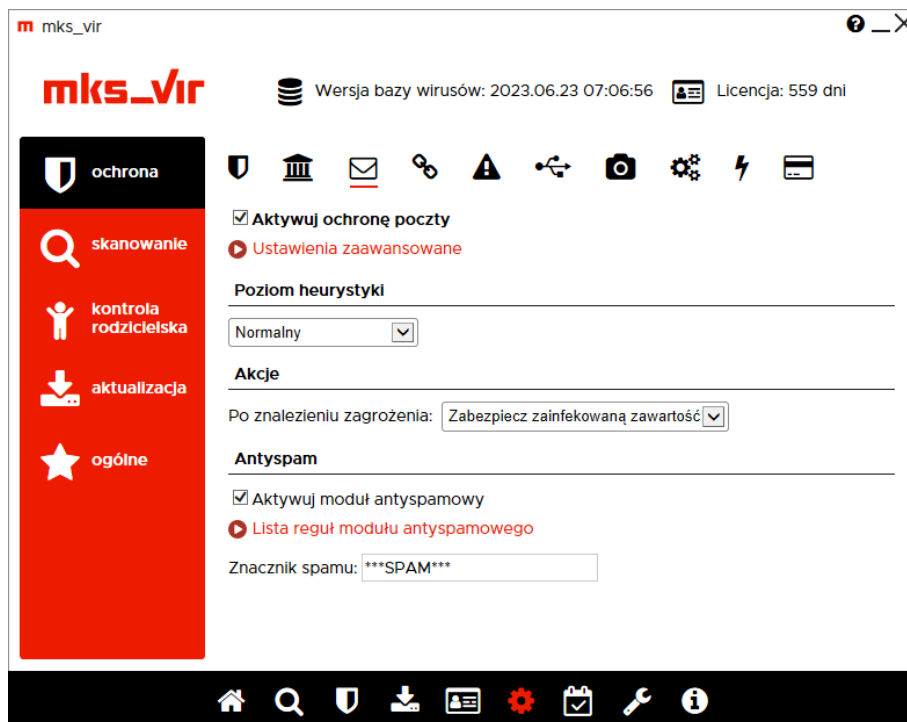
Włącz aktywną ochronę danych SafeStorage – włącza mechanizm ochrony danych, szczególnie przed zagrożeniami szyfrującymi (np. Cryptolocker)

- **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

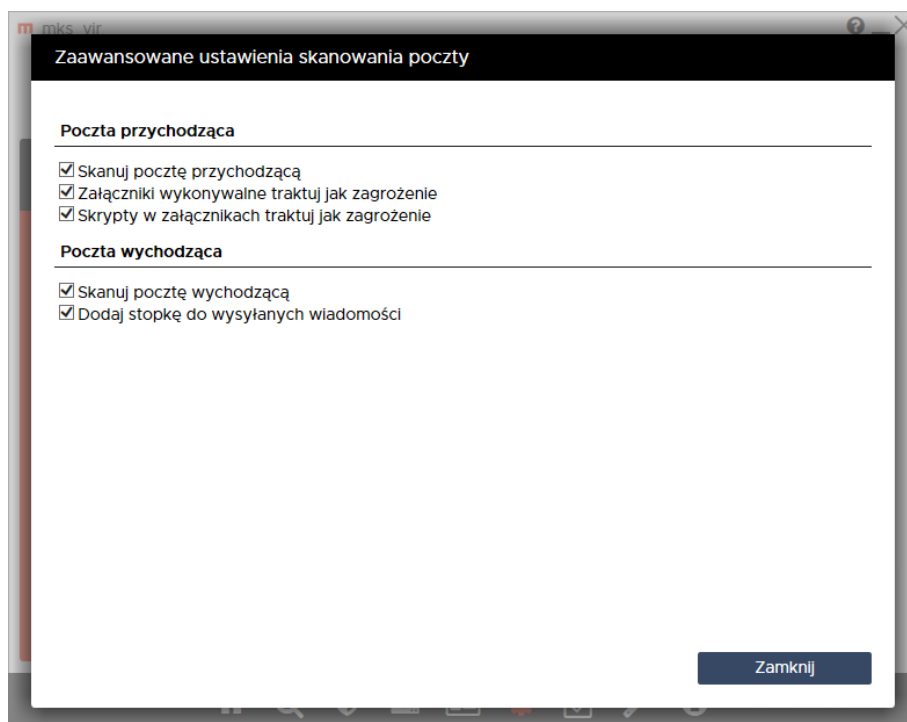
- **Automatycznie wybieraj foldery chronione przez SafeStorage** – przy włączonej opcji program domyślnie chroni dane na wszystkich dyskach lokalnych dostępnych w komputerze; jej wyłączenie umożliwia wybranie, które foldery mają być chronione

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:



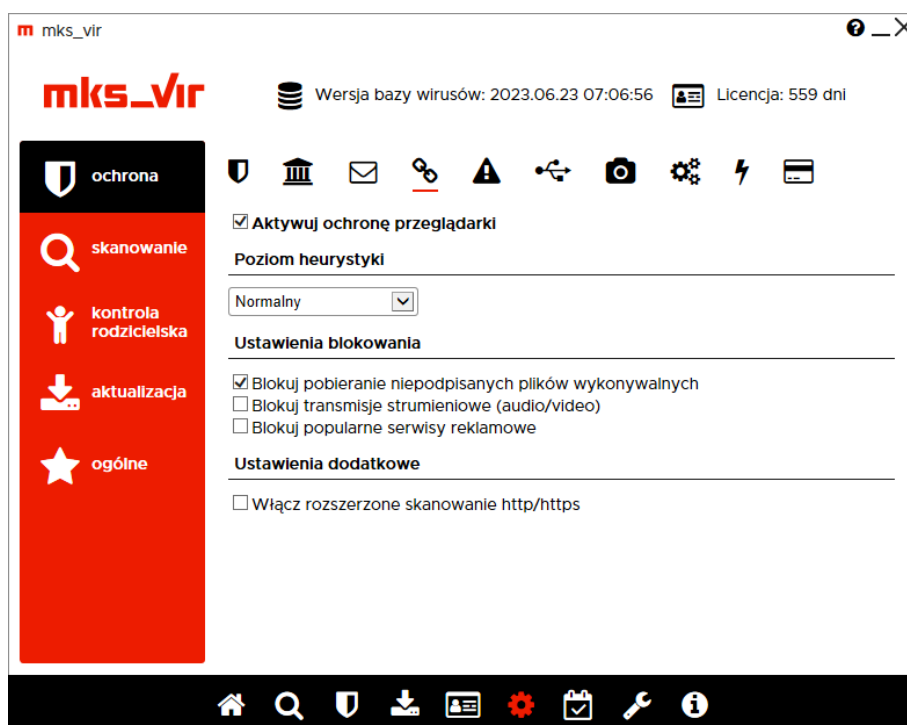
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

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 - oryginalny 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 blokadę 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; aktywacja zapory mks_vir wyłącza zaporę Windows, zaś dezaktywacja zapory mks_vir włącza zaporę Windows, dzięki czemu w systemie stale jest aktywna zaporę
- **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

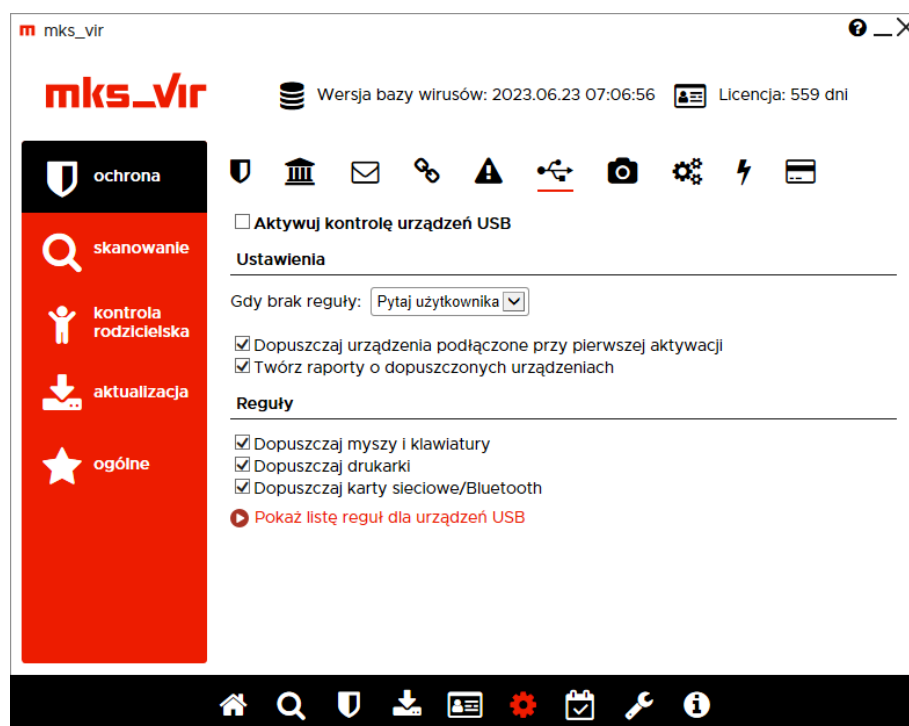
- **Włącz tryb cichy** – włącza tryb działania zapory eliminujący ew. zapytania o przepuszczenie lub zablokowanie połączenia; połączenia dla których pojawiałyby się zapytania będą blokowane
- **Blokuj aktywność sieciową skryptów** – opcja ta blokuje możliwość łączenia się z różnymi witrynami lub pobierania plików, przez różnego rodzaju skrypty (JS, VBS itp.)
- **Blokuj połączenia IPv6** – opcja ta blokuje wszelkie połączenia realizowane przy pomocy protokołu IPv6

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

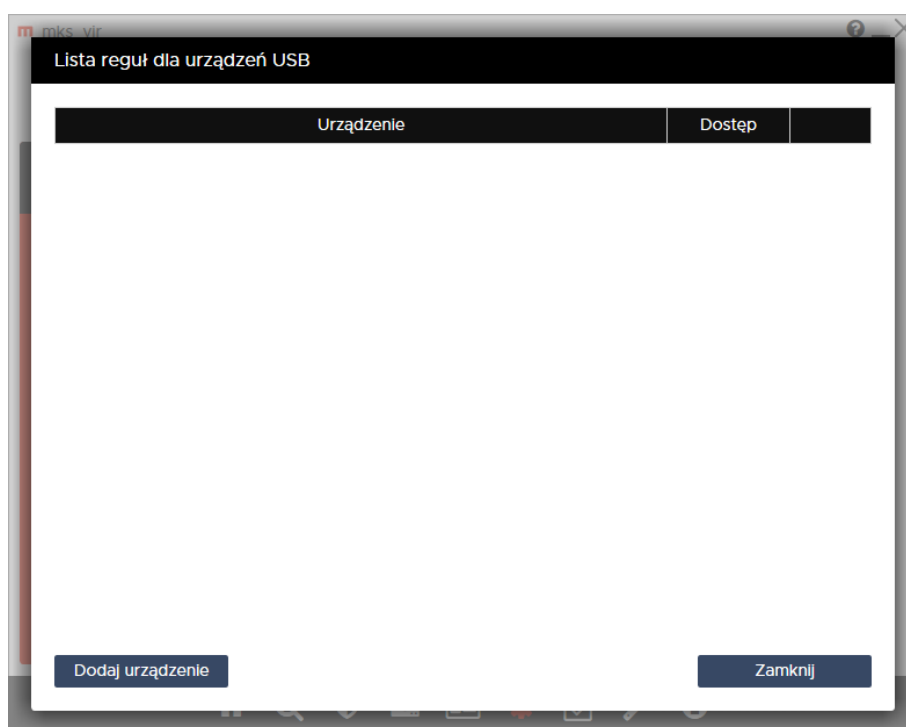
- **Gdy brak reguły** – umożliwia wybranie akcji, która ma być wykonana w przypadku podłączenia nowego urządzenia USB, czyli takiego dla którego nie jest zdefiniowana odpowiednia reguła (dopuszczająca lub blokująca); do wyboru są następujące możliwości:

- **Blokuj** – blokuje każde nowe podłączane urządzenie USB
 - **Dopuszcz** – dopuszcza każde nowe podłączane urządzenie USB
 - **Pytaj użytkownika** – wyświetla okno z pytaniem o zablokowanie lub dopuszczenie nowo podłączanego urządzenia USB; wybranie jednej lub drugiej możliwości tworzy odpowiednią regułę dla danego urządzenia 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 „Dopuszcz” (przy podłączaniu nowych urządzeń USB)

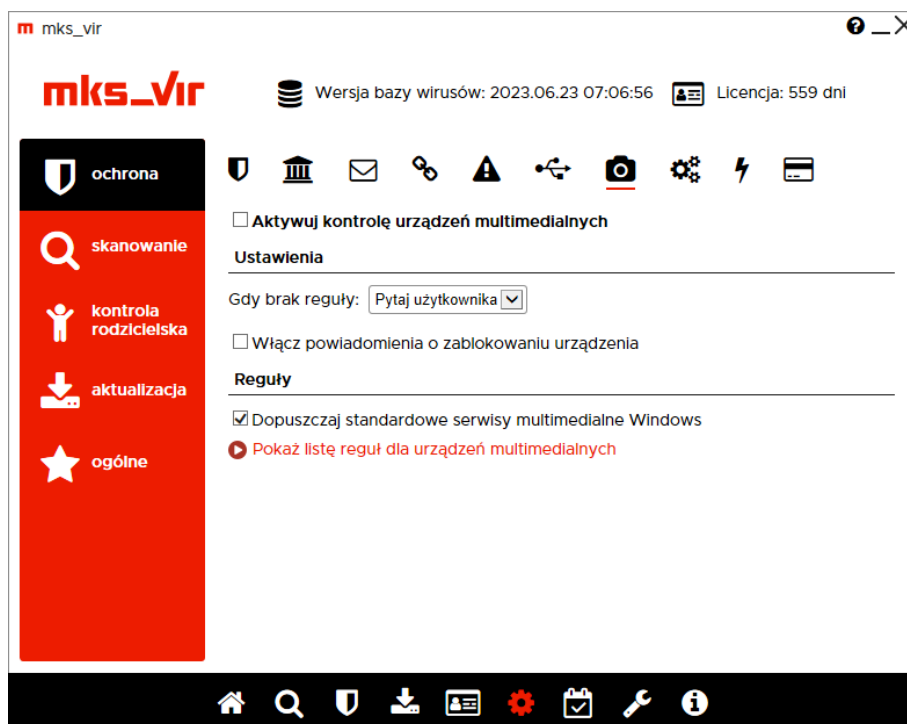
Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających podłączane urządzenia USB

- **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

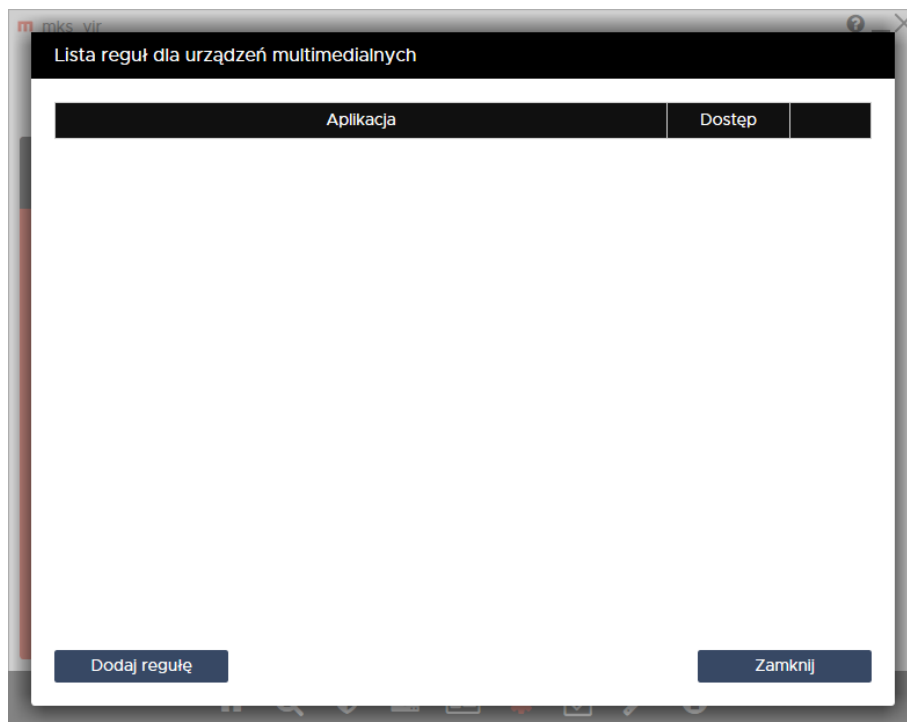
Ustawienia – umożliwia konfigurację modułu kontroli urządzeń multimedialnych

- **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
 - **Dopuszcz** – dopuszcza próbę dostępu do urządzenia multimedialnego przez aplikację
 - **Pytaj użytkownika** – wyświetla okno z pytaniem o dostęp 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”

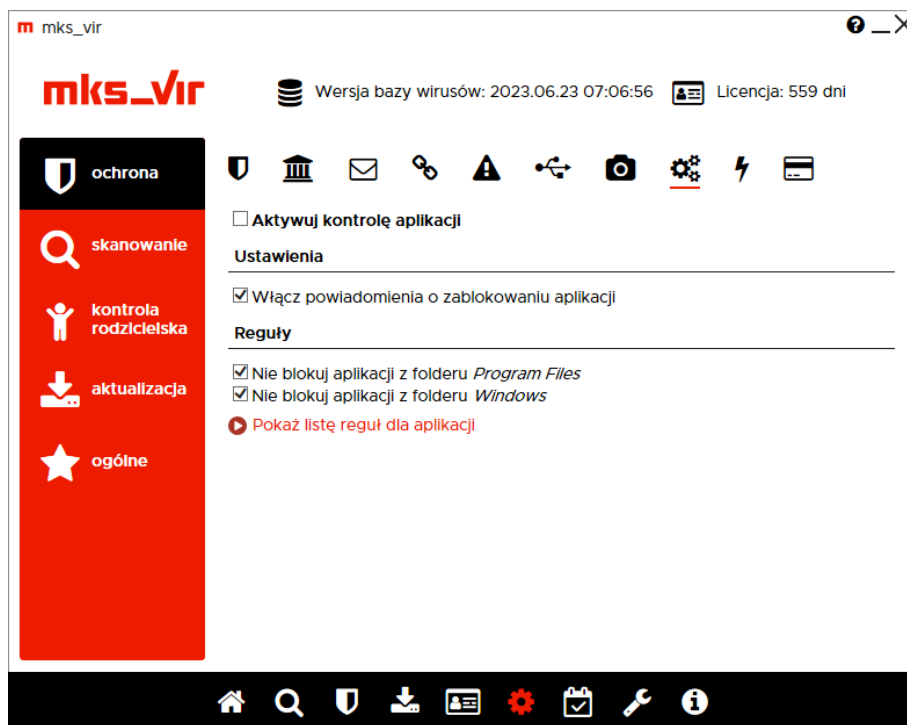
Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających dostęp do urządzeń multimedialnych przez aplikacje

- **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

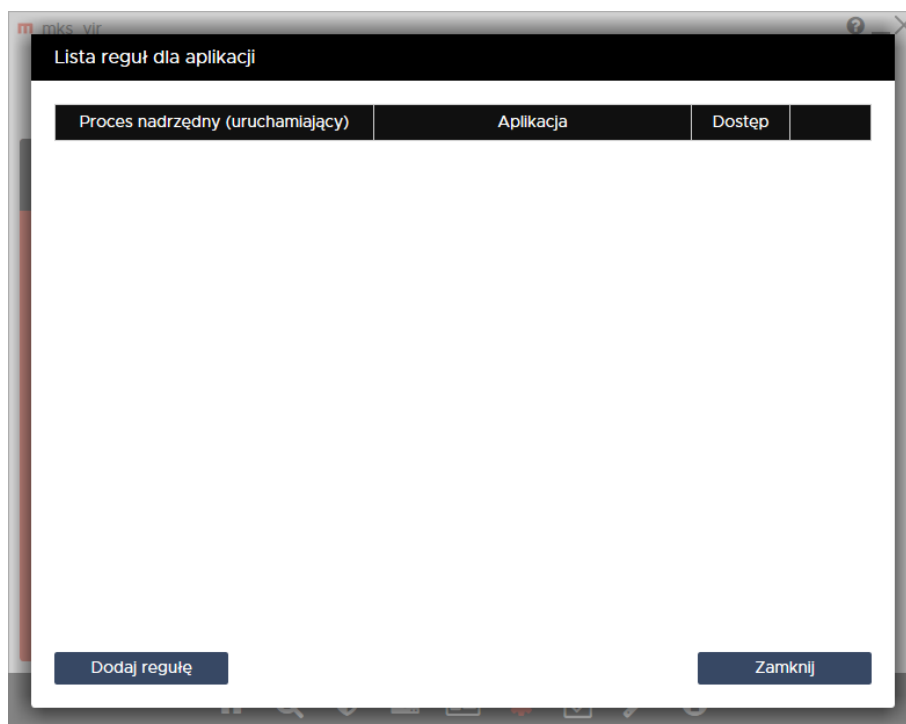
- **Włącz powiadomienia o zablokowaniu aplikacji** – włącza wyświetlanie okien powiadomień modułu kontroli aplikacji w przypadku zablokowania próby uruchomienia aplikacji, dla której została zdefiniowana reguła blokująca

Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających 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!

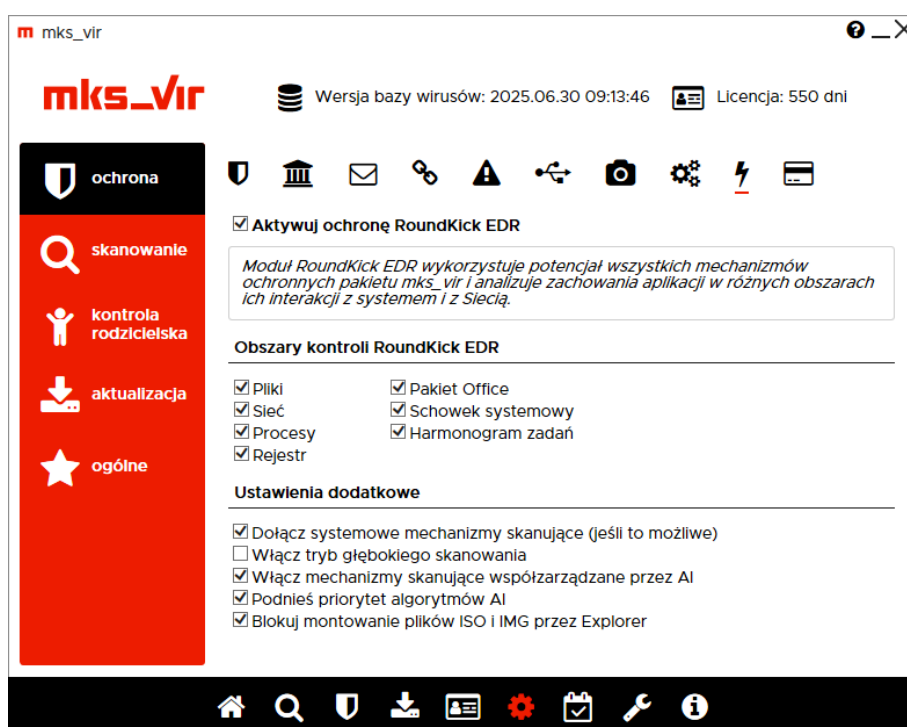
Pokaż listę reguł dla aplikacji – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających uruchamianie aplikacji:



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
- **Harmonogram zadań** – monitoruje zmiany w systemowym harmonogramie zadań, przeprowadzając szczegółową analizę zachowań potencjalnie złośliwych procesów w sposób zintegrowany z usługami chmury obliczeniowej **mks_vir**, wykorzystując mechanizmy uczenia maszynowego i heurystyczne modele detekcji zagrożeń

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

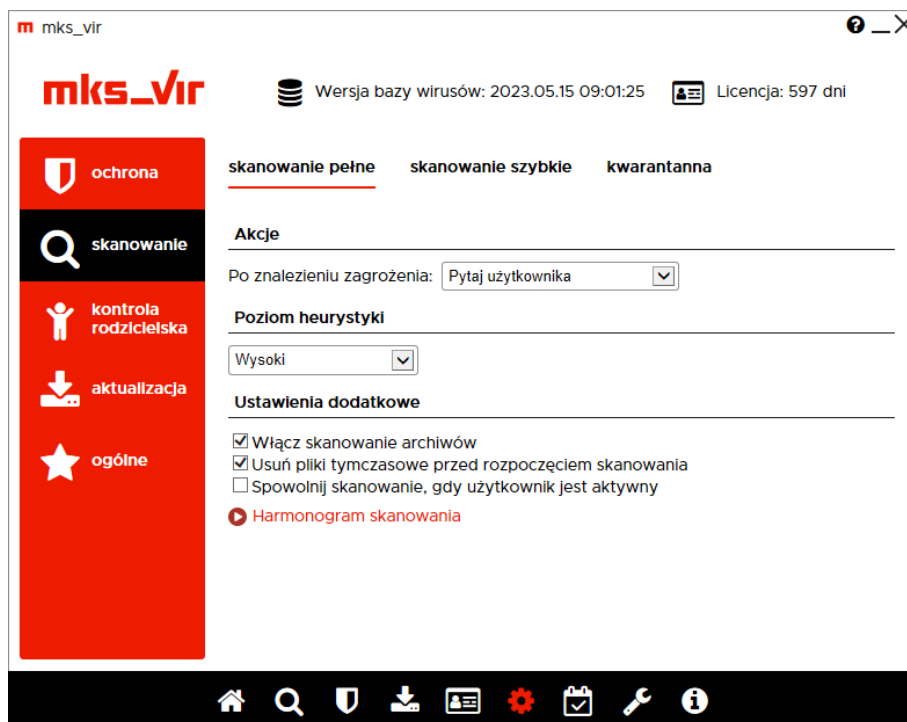
- **Dołącz systemowe mechanizmy skanujące (jeśli to możliwe)** – wyszukuje i wykorzystuje różne moduły skanujące, o ile jakieś są dostępne w systemie
- **Włącz tryb głębokiego skanowania** – włącza zaawansowane mechanizmy skanowania i emulacji celem dokładniejszej analizy skanowanych obiektów
uwaga! włączenie opcji może powodować zauważalne wydłużenie czasów skanowania
- **Włącz mechanizmy skanujące współzarządzane przez AI** – dołączenie do puli mechanizmów skanujących algorytmów i baz zagrożeń zaimplementowanych ze znaczącym udziałem sztucznej inteligencji operującej na dużych zbiorach danych o najnowszych zagrożeniach i wektorach ataków
- **Podnieś priorytet algorytmów AI** – podwyższa priorytet mechanizmów współzarządzanych przez AI w strukturze silników skanujących
- **Blokuj montowanie plików ISO i IMG przez Explorer** – blokuje możliwość montowania obrazów dyskowych typu ISO lub IMG w systemie przez *Ekspłoratora plików* (wiele rodzajów zagrożeń jest przenoszonych w postaci tego typu plików)

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 wykonywana po zakończeniu pełnego skanowania komputera, do wyboru są następujące możliwości:

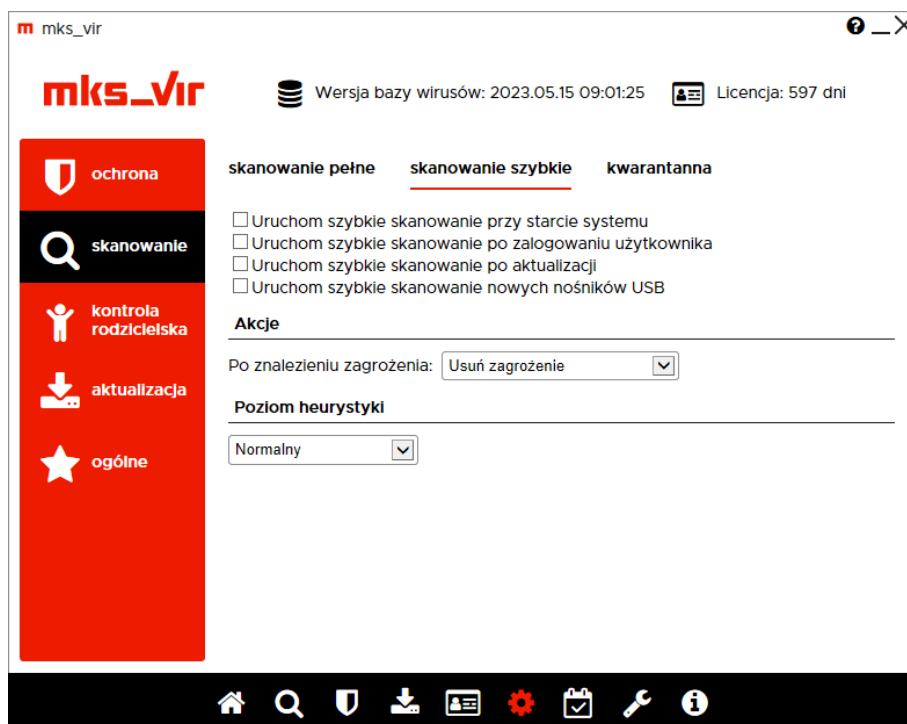
- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Pytaj użytkownika** – po zakończeniu skanowania ew. znalezione zagrożenia zostaną wyświetlone w tabeli z możliwością wyboru akcji, które dla nich będą miały być wykonane

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:

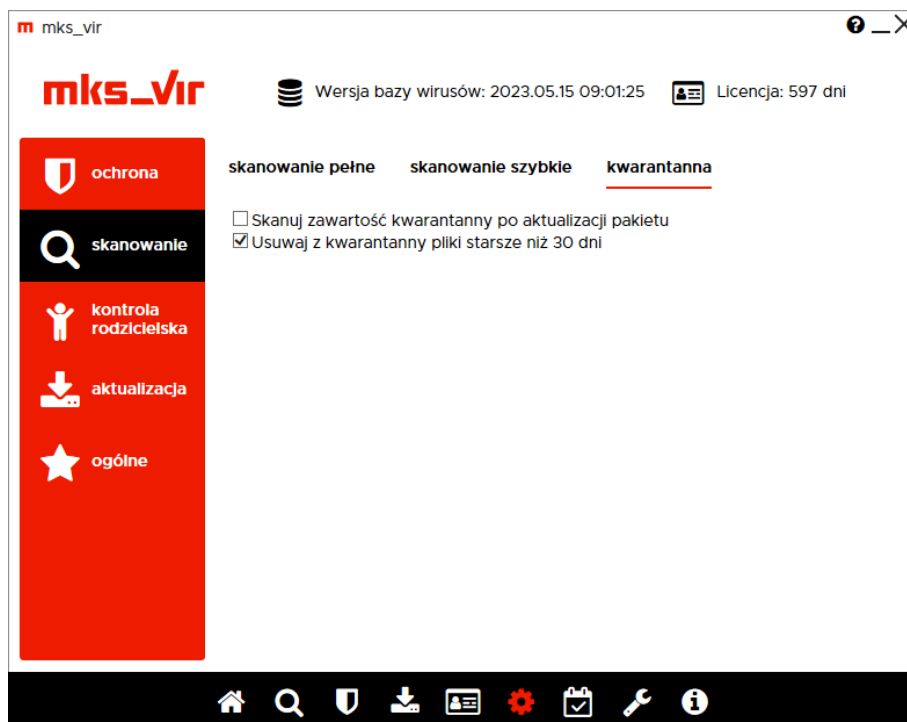
- przy starcie systemu
- po zalogowaniu użytkownika
- po aktualizacji programu mks_vir
- po podłączeniu nośnika USB – skanowana jest wtedy zawartość takiego nośnika

Akcje – umożliwia wybranie akcji, która będzie wykonywana 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**
- **Pytaj użytkownika** – po zakończeniu skanowania ew. znalezione zagrożenia zostaną wyświetlone w tabeli z możliwością wyboru akcji, które dla nich będą miały być wykonane

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

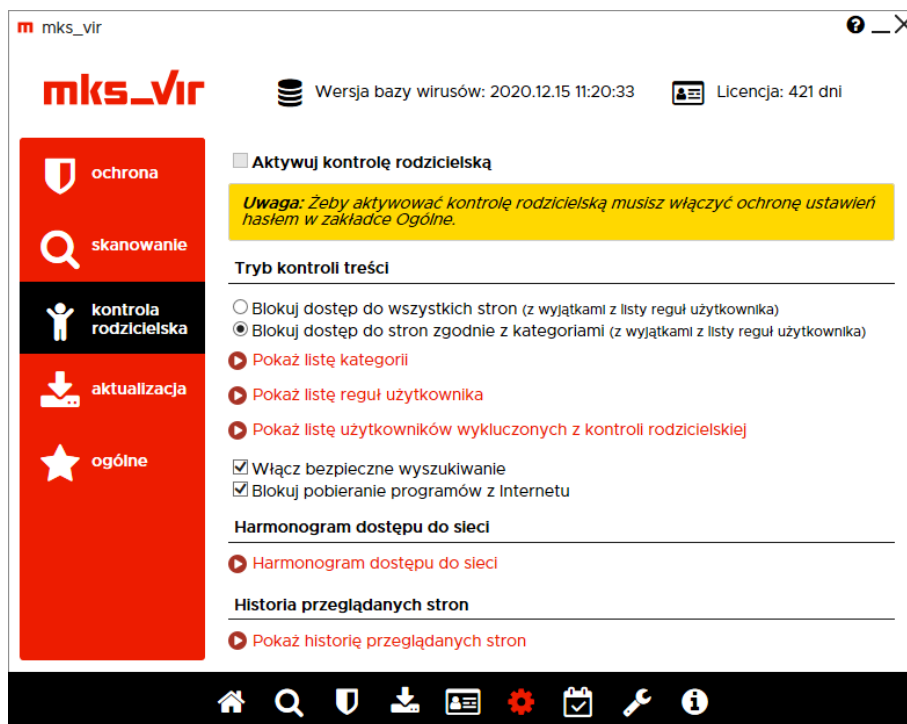
Skanowanie → Kwarantanna:



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 jakiegokolwiek pliki
- **Usuń 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

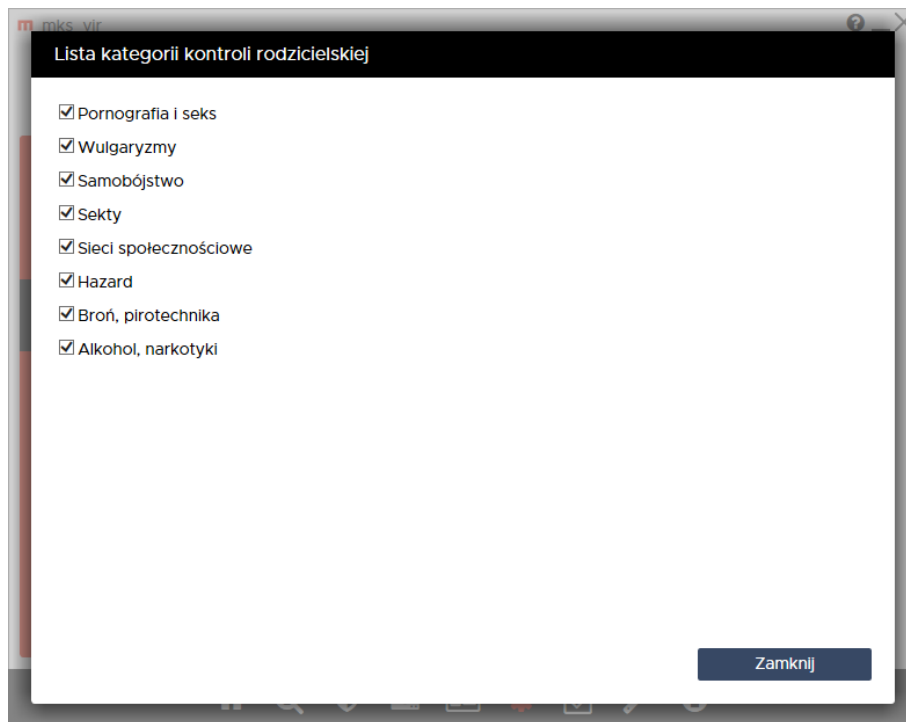
Kontrola rodzicielska:



Aktywuj kontrolę rodzicielską – uaktywnia moduł kontroli rodzicielskiej; aktywacja kontroli rodzicielskiej wymaga wcześniejszego ustawienia ochrony ustawień za pomocą hasła (w sekcji „Ogólne” ustawień)

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 zdefiniowanie własnych reguł przepuszczających lub blokujących w oparciu o adresy lub frazy (słowa kluczowe)

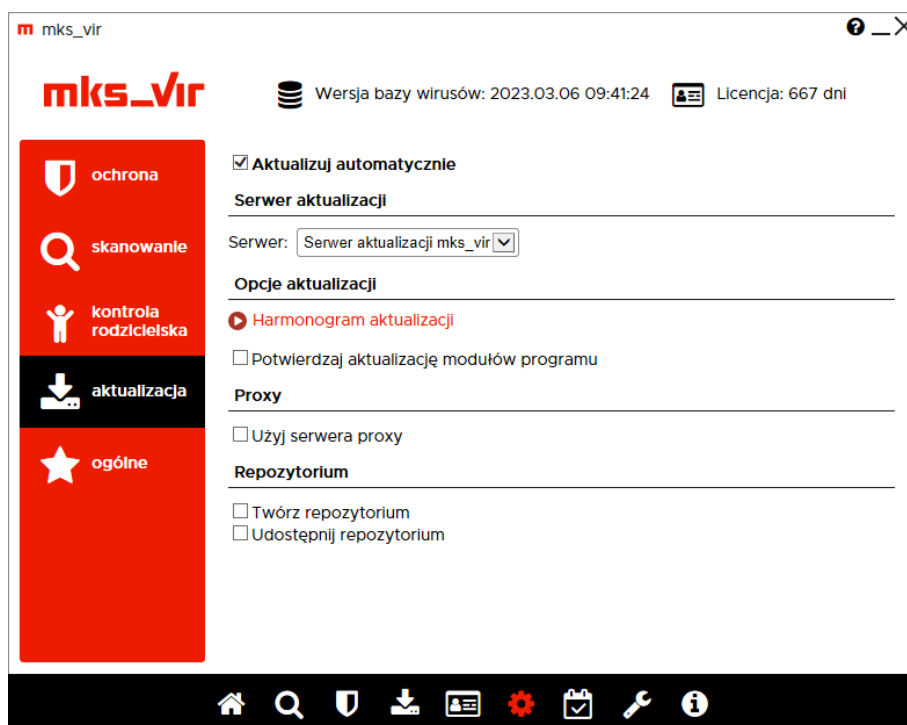
Pokaż listę użytkowników wykluczonych z kontroli rodzicielskiej – umożliwia określenie użytkowników, dla których kontrola rodzicielska będzie zawsze nieaktywna

- **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

Pokaż historię przeglądanych stron – umożliwia przejrzanie adresów stron przeglądanych przez użytkowników oraz zbudowanie na ich podstawie reguł przepuszczających lub blokujących dane strony

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 – umożliwi wybranie źródła aktualizacji, do wyboru są następujące możliwości:

- **Serwer aktualizacji mks_vir** – aktualizacje odbywają się bezpośrednio z serwerów aktualizacyjnych **mks_vir**
- **Inny serwer HTTP** – aktualizacje będą się odbywały z udostępnionego za pomocą protokołu HTTP repozytorium (np. tworzono, 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 – umożliwi określenie, kiedy ma być bezwzględnie wymuszona aktualizacja programu **mks_vir**

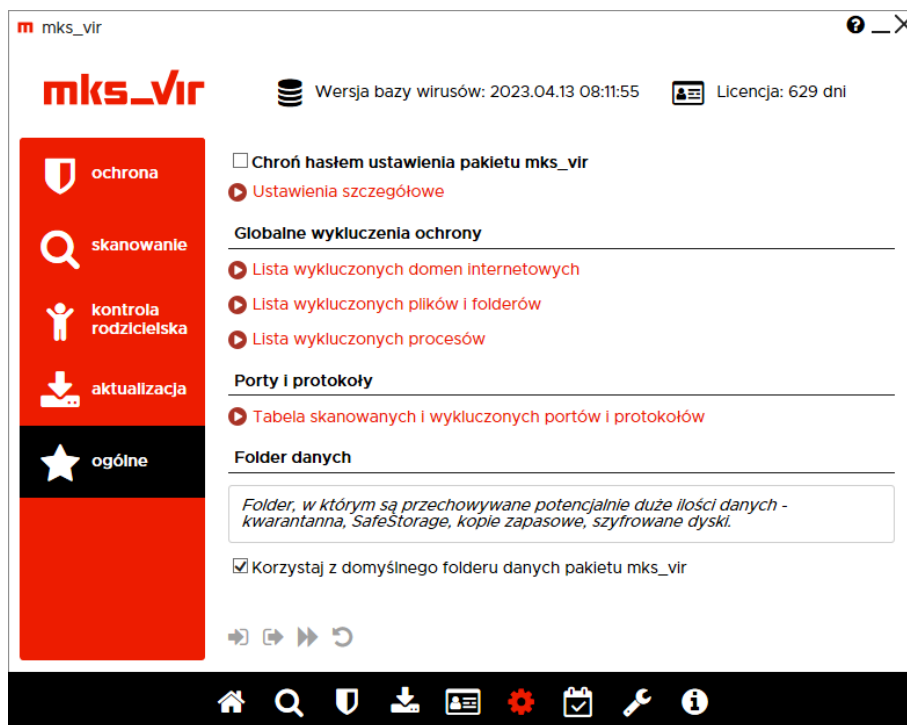
- **Potwierdź aktualizację modułów programu** – włączenie tej opcji powoduje, że na stacjach w przypadku konieczności aktualizacji modułów programowych (a więc innych niż bazy antywirusowe i silniki skanujące) pojawi się pytanie, czy tego dokonać; w niektórych przypadkach samoczynna aktualizacja takich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

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

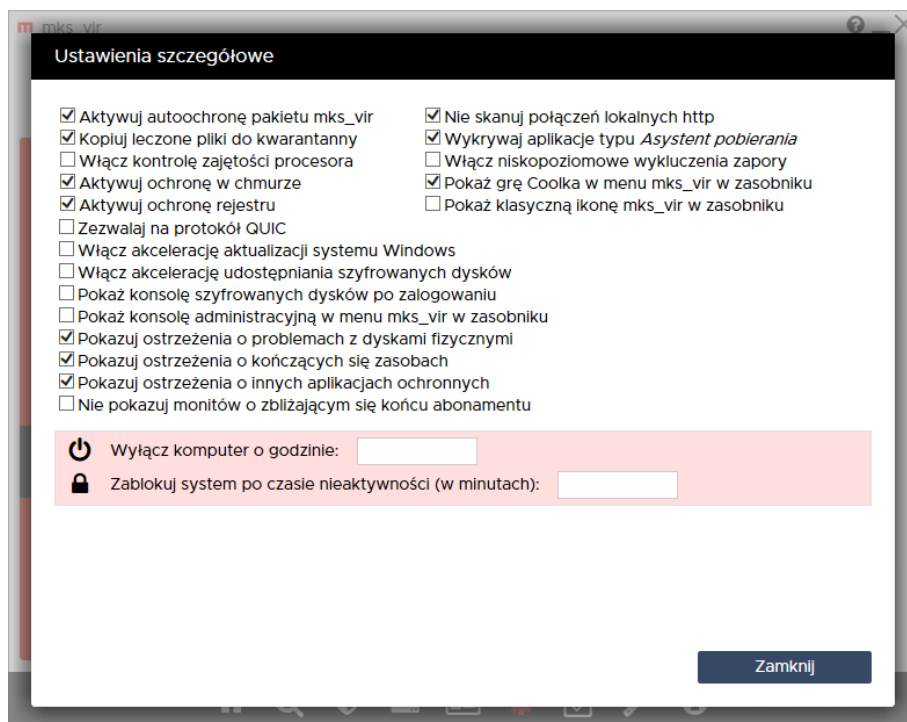
Repozytorium – umożliwi tworzenie, aktualizację i udostępnienie repozytorium w sieci za pomocą protokołu HTTP

- **Twórz repozytorium** – tworzy i aktualizuje repozytorium
- **Udostępnij repozytorium** – umożliwia udostępnienie repozytorium po protokole HTTP na wybranym porcie, który podaje się po włączeniu tej opcji

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 kwarantannie programu **mks_vir** kopie plików leczonych lub kasowanych; funkcja pomocna w przypadku, gdyby była konieczność przywrócenia oryginalnych 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

- **Pokazuj ostrzeżenia o innych aplikacjach ochronnych** – włącza powiadomienia informujące o zainstalowanych i aktywnych w systemie innych aplikacjach ochronnych (antywirusowych), co może być potencjalnym źródłem spadku wydajności, konfliktów z różnymi programami, a nawet destabilizacji pracy systemu
- **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:

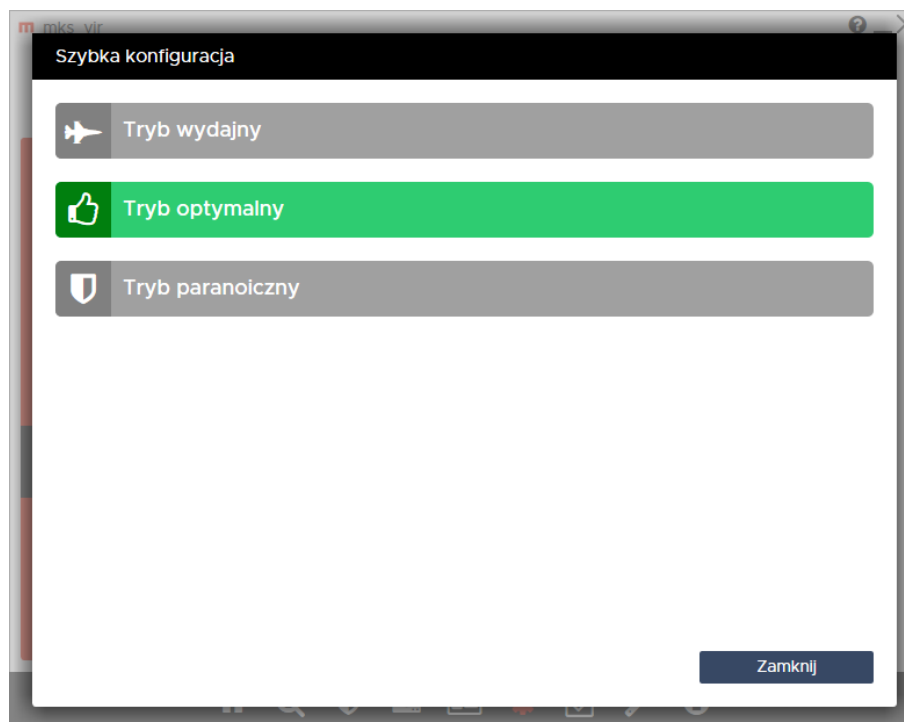
- **Lista wykluczonych domen internetowych** – umożliwia zdefiniowanie adresów, dla których nie będą działały moduły ochrony przeglądarki i kontroli rodzicielskiej programu **mks_vir**
- **Lista wykluczonych plików i folderów** – umożliwia zdefiniowanie obiektów (plików lub folderów), dla których nie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

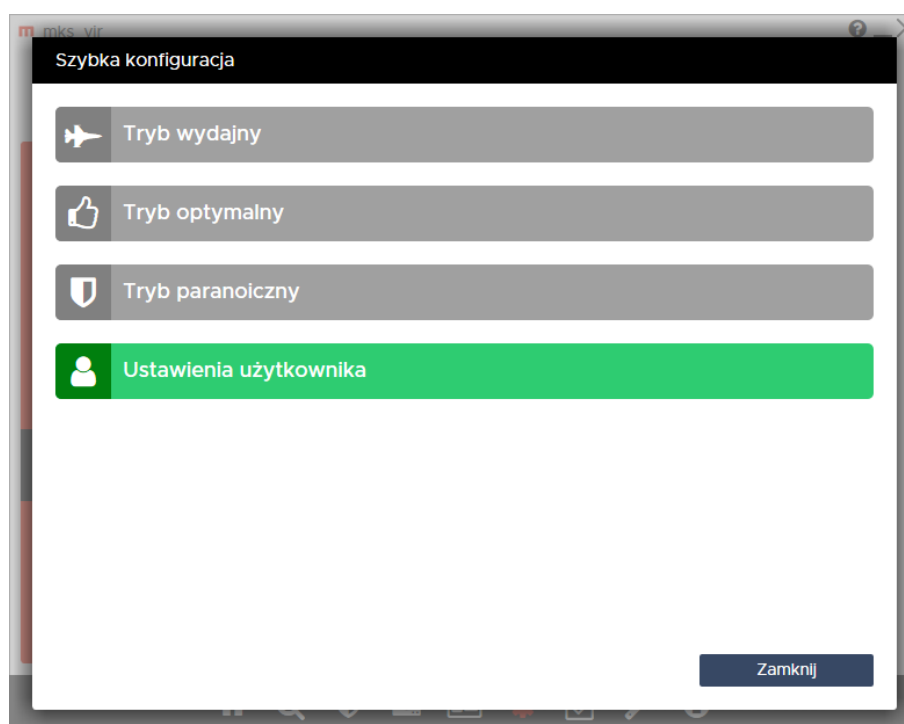
Folder danych – umożliwia określenie innego niż domyślny folderu dla dużych ilości danych (kwarantanna, *SafeStorage*, kopie zapasowe, szyfrowane dyski); zdefiniowanie innego niż domyślny folderu wymaga, by dysk twardy na którym ma się znajdować, był dostępny w komputerze

- ➔ – 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

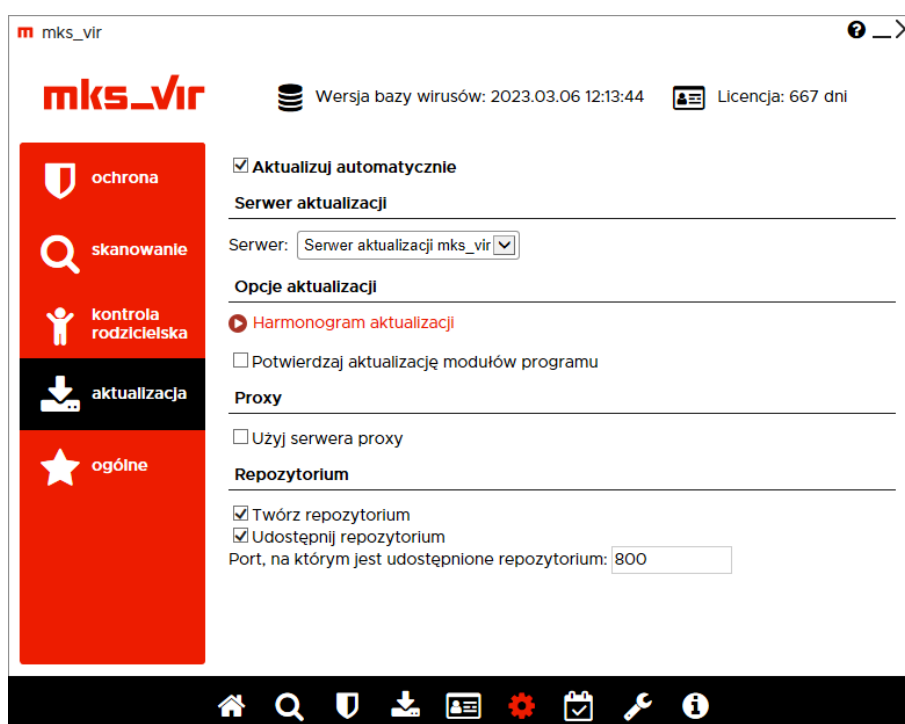


↺ – przywraca domyślną konfigurację programu **mks_vir** (*przywróć ustawienia domyślne*)

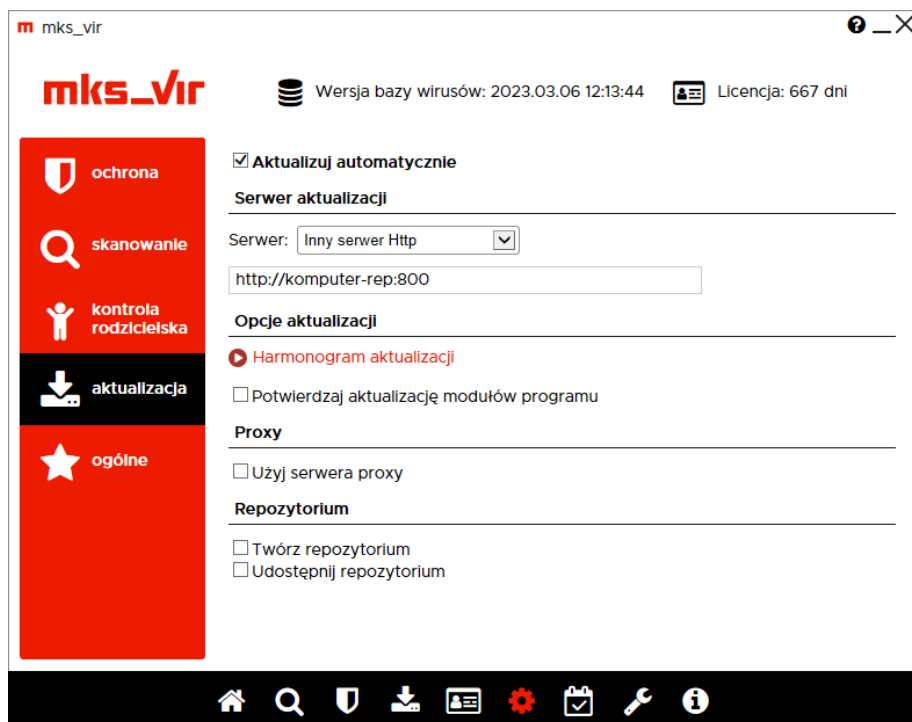
Aktualizacja programu w sieciach lokalnych za pomocą mechanizmu repozytorium udostępnianego po HTTP

Aby uaktualnić instalacje programu **mks_vir** w sieciach lokalnych przez mechanizm repozytorium udostępnianego po protokole HTTP należy:

- Na jakiejś maszynie z dostępem do Internetu i zainstalowanym programem **mks_vir** na licencji wielostanowiskowej tworzymy tzw. repozytorium, czyli:
 1. klikamy lewym klawiszem myszy w ikonę **mks_vir** na pasku zadań
 2. w głównym oknie programu wybieramy „Ustawienia → Aktualizacja”
 3. zaznaczamy opcje „Twórz repozytorium” i „Udostępnij repozytorium” oraz wpisujemy port np. 800:



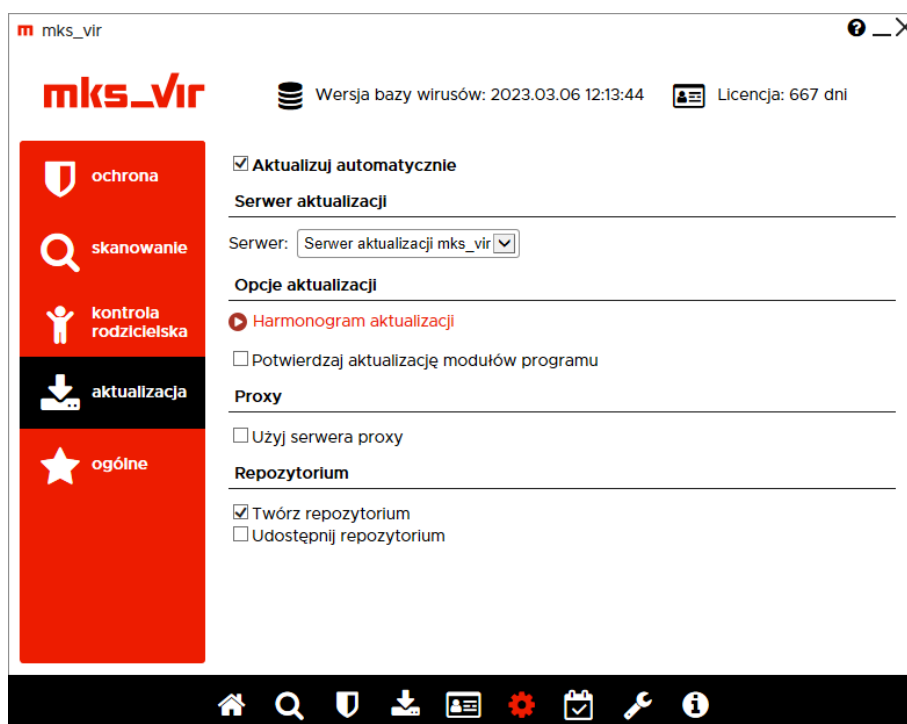
- Na maszynach które mają się uaktualniać z takiego repozytorium ustawiamy:
 1. klikamy lewym klawiszem myszy w ikonę **mks_vir** na pasku zadań
 2. w głównym oknie programu wybieramy „Ustawienia → Aktualizacja”
 3. wybieramy serwer „Inny serwer HTTP” i wpisujemy adres sieciowy komputera, który tworzy i udostępnia repozytorium wraz z numerem portu, na którym jest udostępniane repozytorium (w formacie `http://adres_komputera:port`):



Aktualizacja programu na stacjach bez dostępu do sieci za pomocą mechanizmu repozytorium

Aby uaktualnić instalacje programu **mks_vir** na stacjach bez dostępu do sieci za pomocą mechanizmu repozytorium przenieszonego na płytce CD/DVD lub pamięci Flash należy:

- Na jakiejś maszynie z dostępem do Internetu i zainstalowanym programem **mks_vir** na licencji wielostanowiskowej tworzymy tzw. repozytorium, czyli:
 1. klikamy lewym klawiszem myszy w ikonę **mks_vir** na pasku zadań
 2. w głównym oknie programu wybieramy „Ustawienia → Aktualizacja”
 3. zaznaczamy opcję „Twórz repozytorium”:

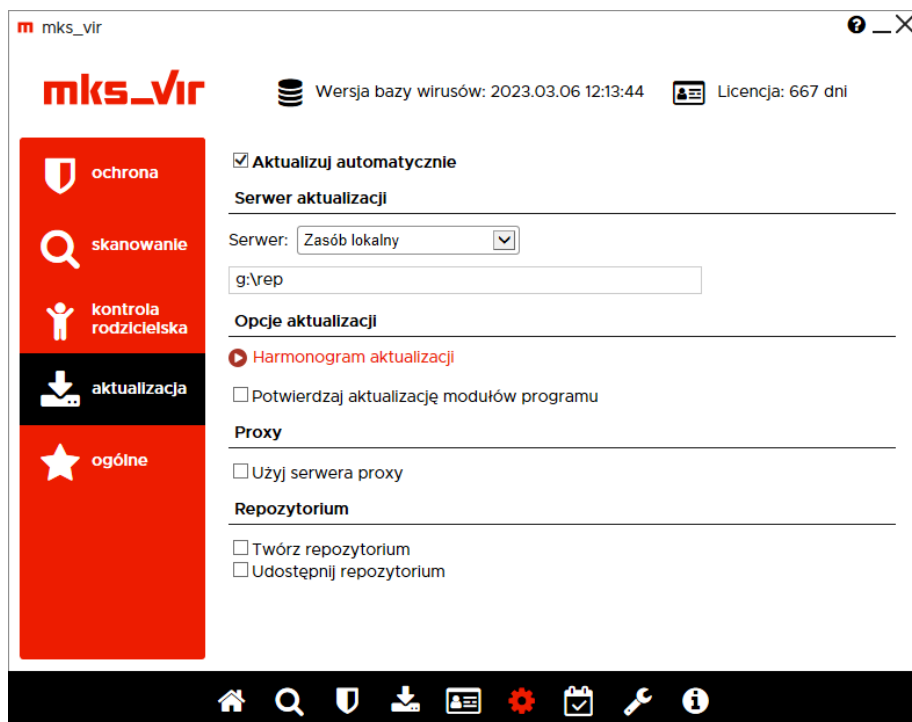


4. Repozytorium tworzone jest w folderze:

- w systemach Windows XP i Windows Server 2003/2003R2:
c:\documents and settings\all users\mks_vir\repository
- w systemach Windows Vista/7/8/8.1/10/11
i Windows Server 2008/2008R2/2012/2012R2/2016/2019/2022:
c:\programdata\mks_vir\repository

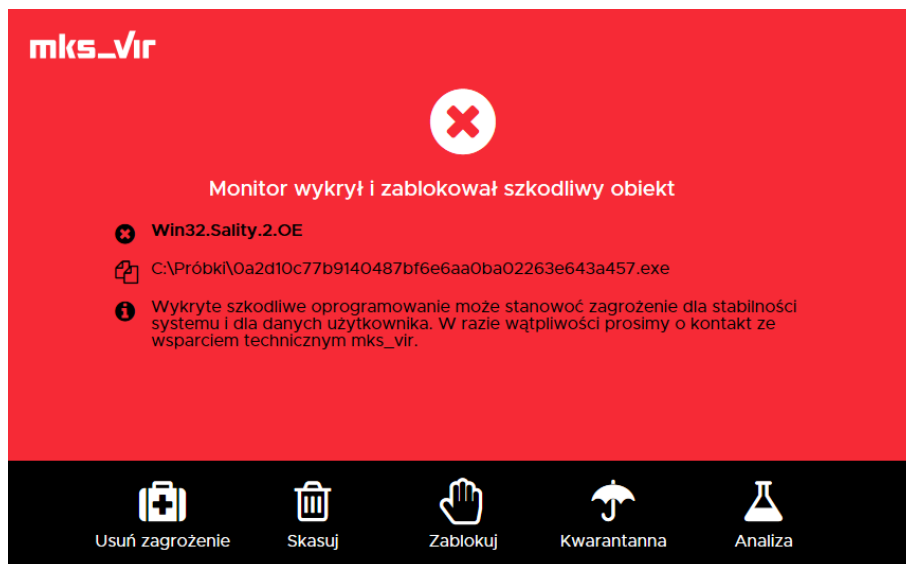
Zawartość tego folderu należy skopiować na płytę CD/DVD lub pamięć Flash.

- Na maszynach które mają się uaktualniać z takiego repozytorium ustawiamy:
 1. klikamy lewym klawiszem myszy w ikonę **mks_vir** na pasku zadań
 2. w głównym oknie programu wybieramy „Ustawienia → Aktualizacja”
 3. wybieramy serwer „Zasób lokalny” i wpisujemy wpisujemy dysk, z którego chcemy aktualizować program (np. „G:”, a jeśli repozytorium znajduje się w podkatalogu wpisujemy razem z nazwą podkatalogu, np. „G:\rep”):



Sygnalizacja wykrycia zagrożenia przez moduł „Ochrona plików”

W przypadku, gdy program **mks_vir** wykryje coś, co zakwalifikuje jako **zagrożenie**, okno wykrycia wygląda następująco:

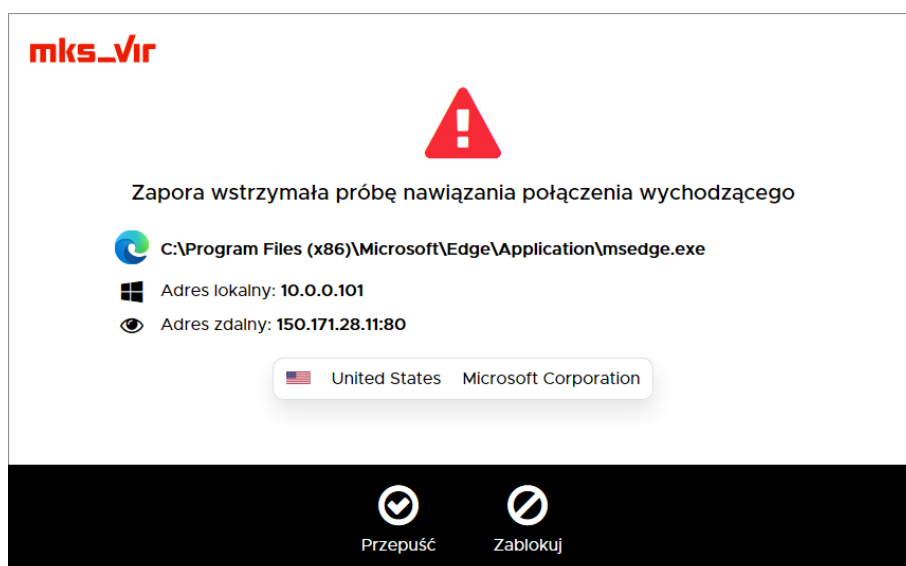


Dostępne do wyboru są następujące akcje:

- **Usuń zagrożenie** – leczy plik, jeśli zagrożenie jest wirusem lub kasuje, jeśli zagrożenie jest inne (trojan, robak itp.)
- **Skasuj** – niezależnie od tego, czy to plik zarażony wirusem, czy jest to inne zagrożenie, plik jest kasowany bez możliwości jego odzyskania
- **Zablokuj** – plik zostaje zablokowany i chociaż pozostaje na dysku, nie jest dostępny dla użytkownika
- **Kwarantanna** – plik jest szyfrowany (aby nie stanowił zagrożenia) i przenoszony do specjalnego folderu; w razie potrzeby plik z kwarantanny można odzyskać
- **Analiza** – wybranie tej możliwości pozwala na wysłanie pliku do działu analiz **mks_vir** w celu dokładniejszej analizy, np. w przypadku, gdy użytkownik nie zgadza się z klasyfikacją pliku przez program antywirusowy

Sygnalizacja próby połączenia przez moduł „Zapory”

Gdy aktywny jest moduł „Zapory” program **mks_vir** może sygnalizować próby połączeń sieciowych przez aplikacje:



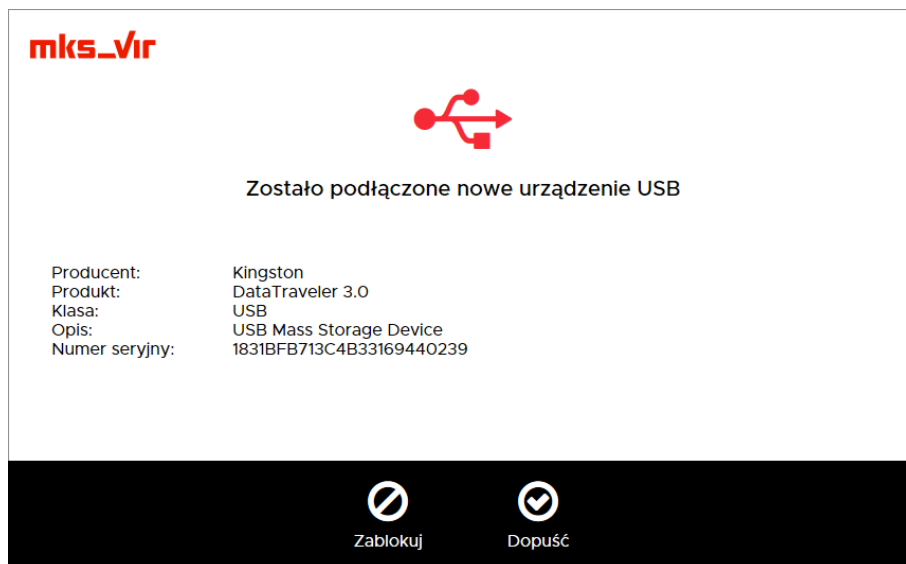
W przypadku pojawienia się tego typu komunikatu są do wyboru dwie możliwości:

- **Przepuść** – zezwala na nawiązanie sygnalizowanego połączenia przez aplikację wyświetlaną w tym oknie
- **Zablokuj** – nie zezwala na nawiązanie połączenia przez aplikację wyświetlaną w tym oknie

W obu przypadkach tworzone są automatycznie reguły dla „Zapory” programu **mks_vir**, dzięki czemu komunikaty dotyczące danej aplikacji nie będą się powtarzały. Tak utworzone reguły można modyfikować w „Ustawieniach” programu **mks_vir**, w sekcji „Ochrona → Zapora → Reguły zapory sieciowej”

Sygnalizacja podłączenia urządzenia USB przez moduł „Kontroli urządzeń USB”

Gdy aktywny jest moduł „Kontroli urządzeń USB” program **mks_vir** może sygnalizować próby podłączenia różnych urządzeń do portów USB komputera:



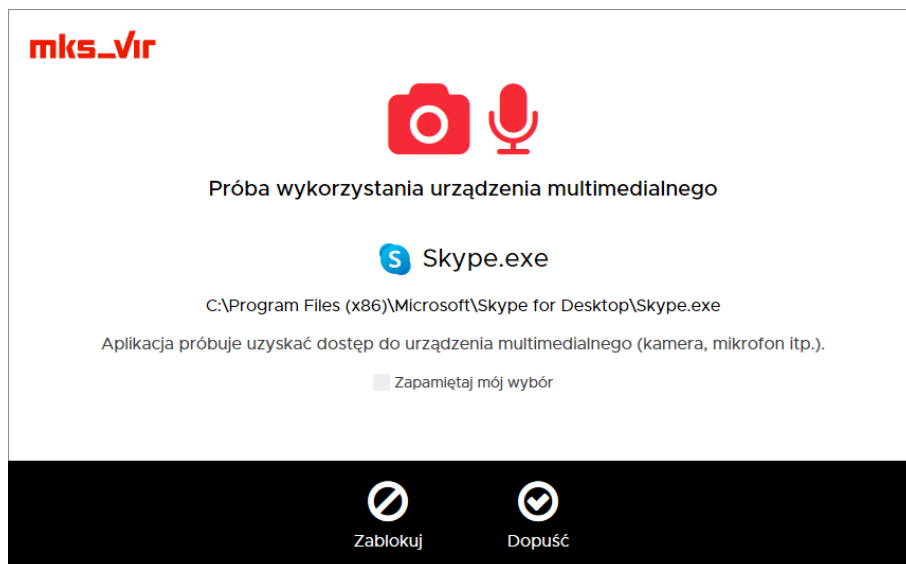
W przypadku pojawienia się tego typu komunikatu są do wyboru dwie możliwości:

- **Zablokuj** – nie zezwala na podłączenie urządzenia USB do komputera
- **Dopuszcz** – zezwala na podłączenie urządzenia USB do komputera

W obu przypadkach tworzone są automatycznie reguły dla „Kontroli urządzeń USB” programu **mks_vir**, dzięki czemu komunikaty dotyczące danego urządzenia (w przypadku jego odłączenia i ponownego podłączenia) nie będą się powtarzały. Tak utworzone reguły można modyfikować w „Ustawieniach” programu **mks_vir**, w sekcji „Ochrona → Kontrola urządzeń USB → Pokaż listę reguł dla urządzeń USB”

Sygnalizacja dostępu aplikacji do urządzenia multimedialnego przez moduł „Kontroli urządzeń multimedialnych”

Gdy aktywny jest moduł „Kontroli urządzeń multimedialnych” program **mks_vir** może sygnalizować próby dostępu różnych aplikacji do urządzeń multimedialnych komputera:



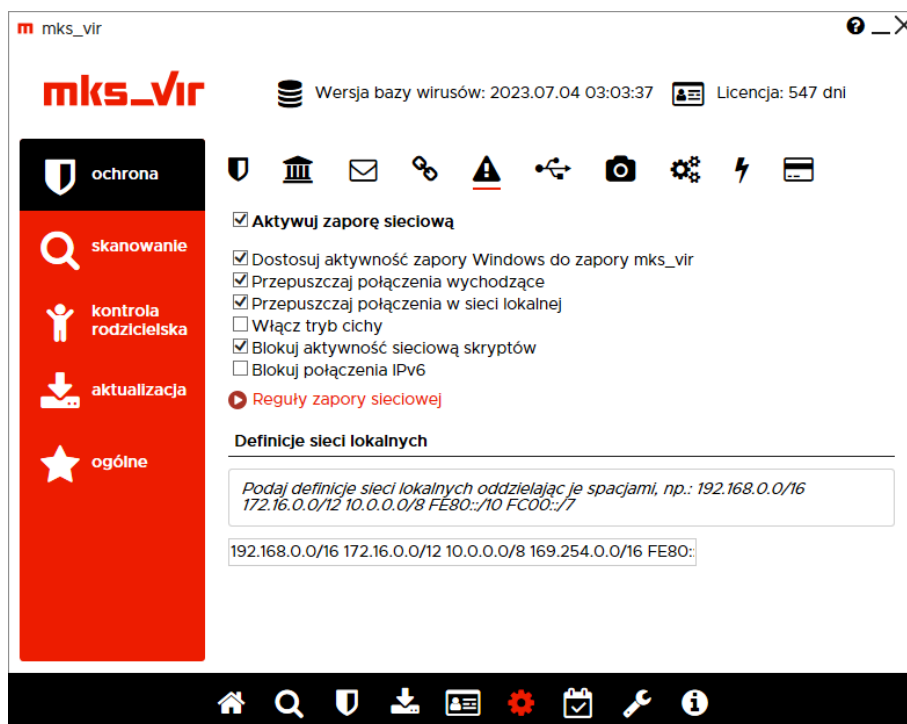
W przypadku pojawienia się tego typu komunikatu są do wyboru dwie możliwości:

- **Zablokuj** – nie zezwala na dostęp do urządzenia multimedialnego przez aplikację
- **Dopuszcz** – zezwala na dostęp do urządzenia multimedialnego przez aplikację

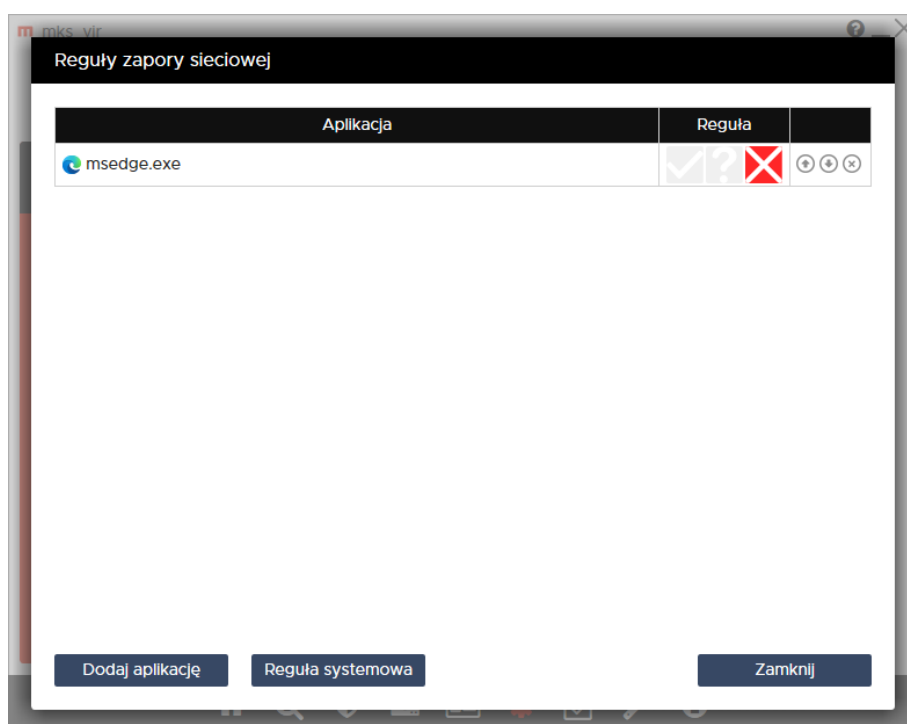
Jeśli przed wybraniem akcji zaznaczymy „Zapamiętaj mój wybór”, to zostanie utworzona reguła dopuszczająca lub blokująca na stałe dostęp aplikacji do urządzeń multimedialnych, dzięki czemu komunikaty dotyczące danej aplikacji nie będą się powtarzały. Tak utworzone reguły można modyfikować w „Ustawieniach” programu **mks_vir**, w sekcji „Ochrona → Kontrola urządzeń multimedialnych → Pokaż listę reguł dla urządzeń multimedialnych”

Jak odblokować aplikację zablokowaną w „Zaporze”

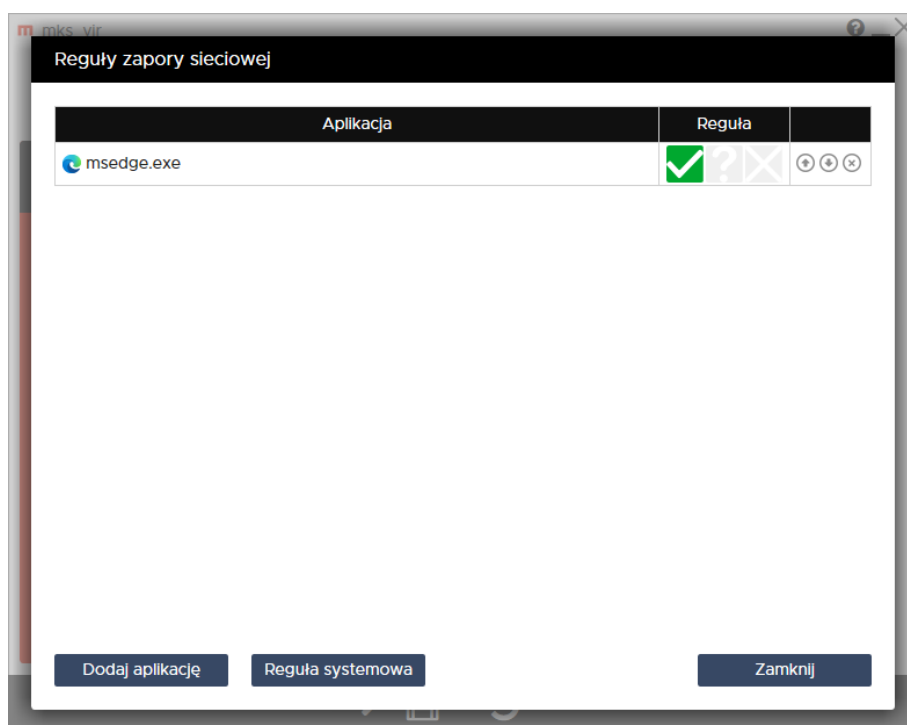
Aby odblokować aplikację, która została wcześniej zablokowana w „Zaporze” programu mks_vir na skutek wyświetlenia komunikatu i wybrania akcji „Blokuj”, należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do sekcji „Ochrona → Zapora sieciowa (firewall)”:



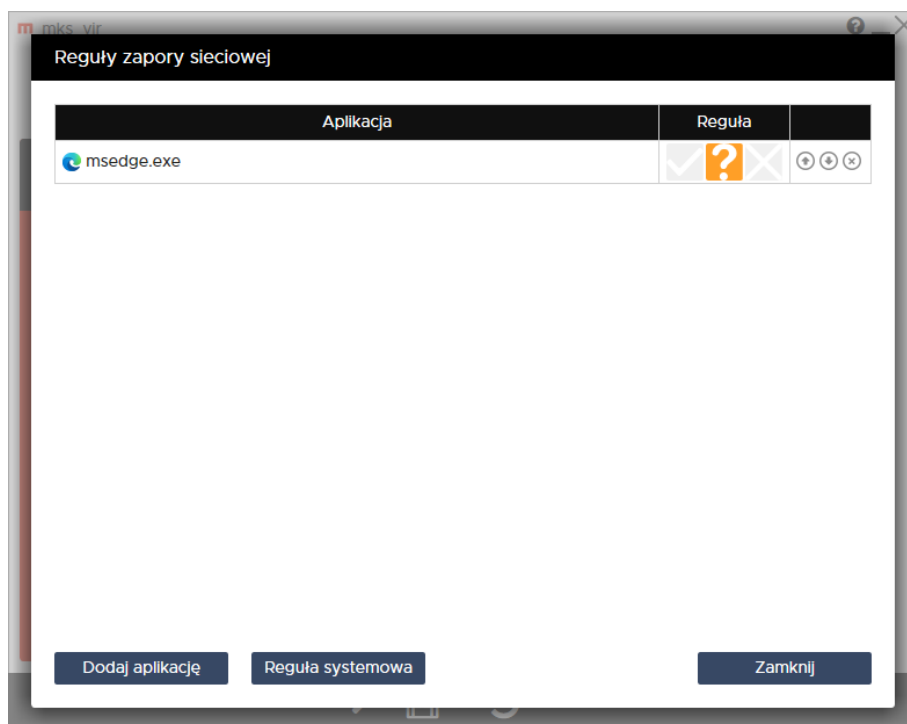
Po wybraniu „Reguły zapory sieciowej” pojawi się okno z aktualnymi regułami zapory sieciowej. Aplikacja, która została zablokowana przez „Zaporę” oznaczona jest na czerwono w kolumnie „Reguła”:



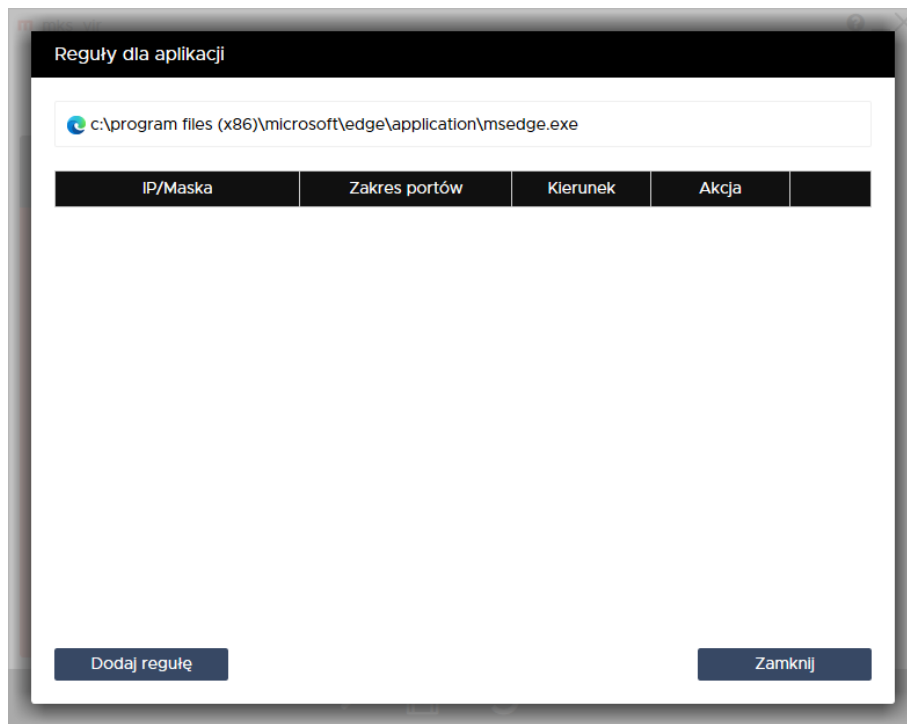
Aby szybko odblokować taką aplikację, wystarczy kliknąć pierwszy znak w kolumnie „Reguła” (zielony oznacza regułę przepuszczającą):



Jeśli jednak chcemy dokładniej określić warunki określające działanie połączeń sieciowych dla danej aplikacji, należy kliknąć w środkowy znak w kolumnie „Reguła”:

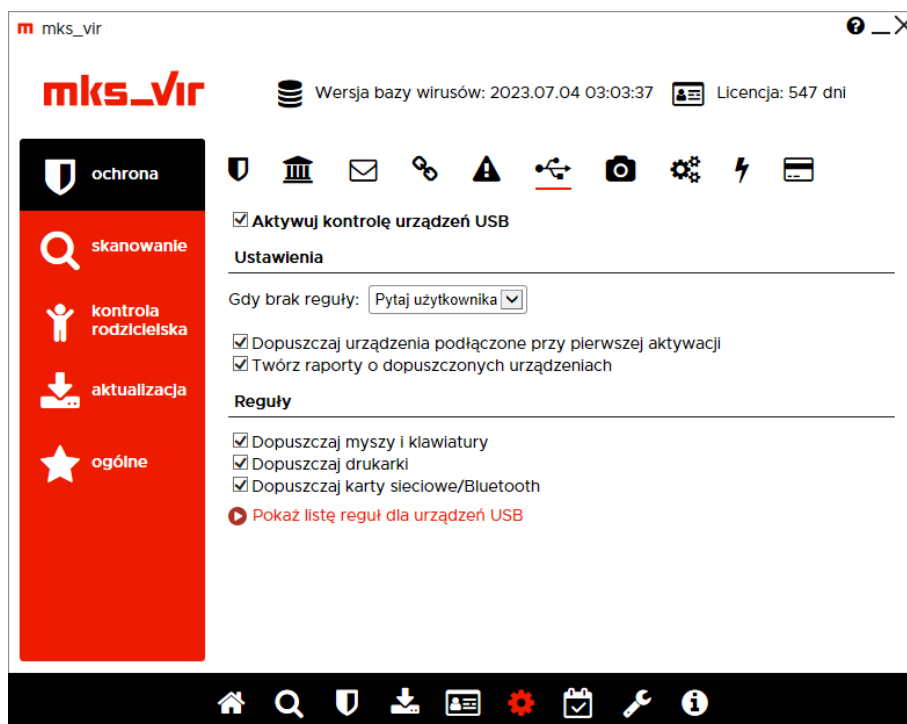


Otworzy się wówczas okno, gdzie możemy dokładnie zdefiniować reguły, dla których dana aplikacja ma być przepuszczana lub blokowana:

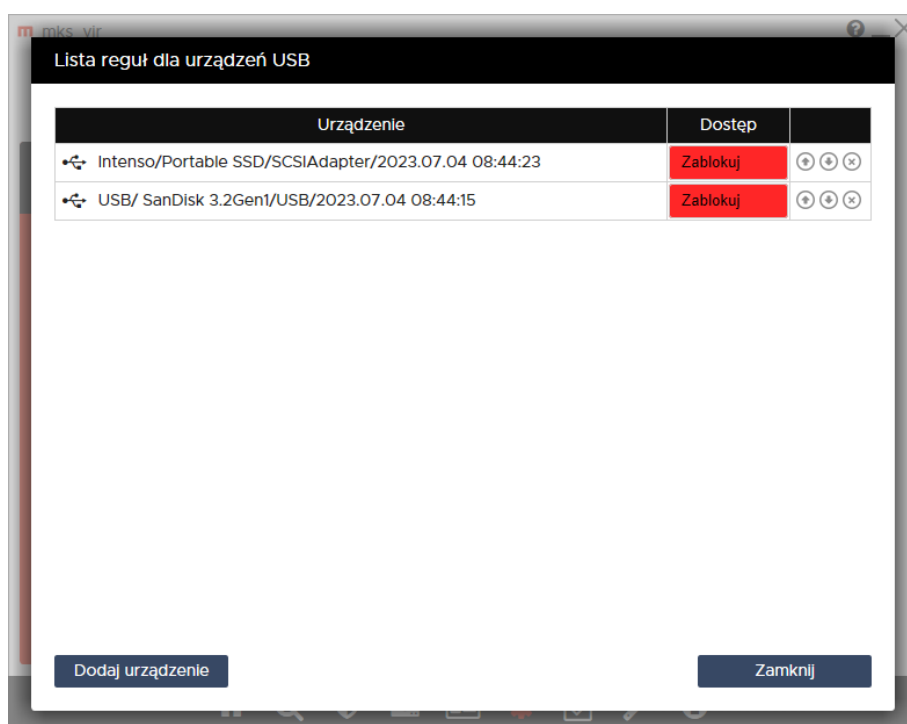


Jak zmodyfikować regułę w module „Kontrola urządzeń USB”

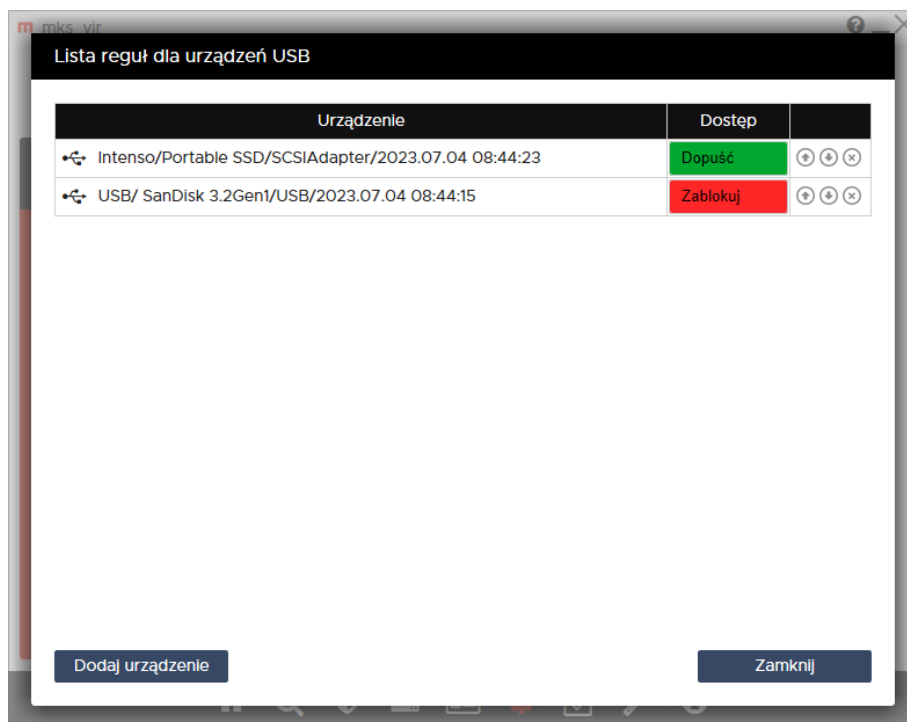
Aby zmodyfikować regułę utworzoną wcześniej w module „Kontrola urządzeń USB” programu **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do „Ochrona → Kontrola urządzeń USB → Pokaż listę reguł dla urządzeń USB”



Modyfikując utworzoną regułę przede wszystkim można zmienić tryb dostępu do danego urządzenia, np. z akcji „Zablokuj” (czyli nie zezwalającej na użycie danego urządzenia):



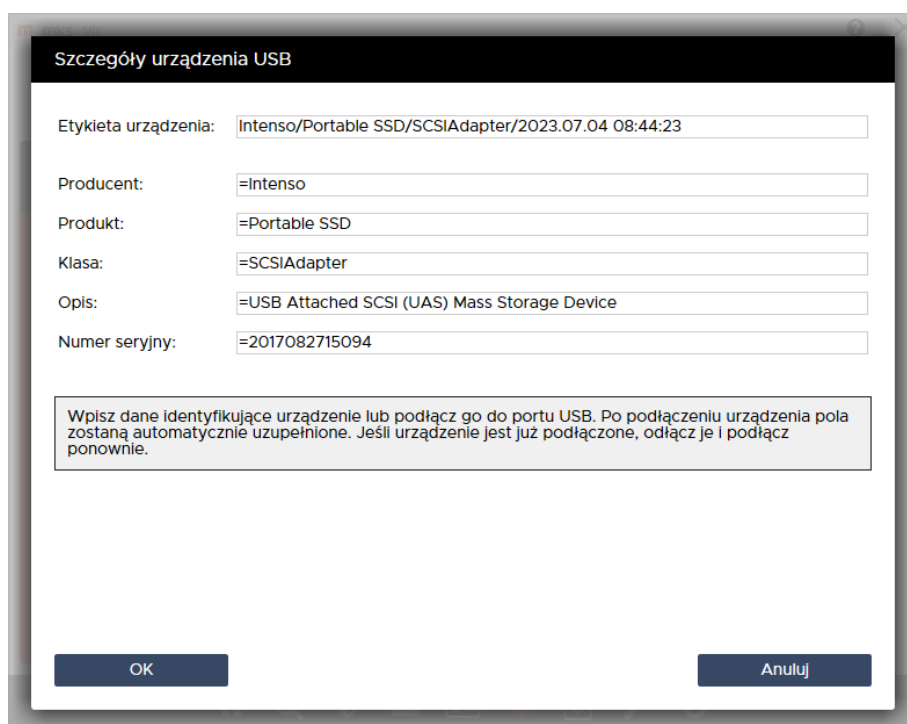
na akcję „Dopuszcz” (czyli zezwalającą na użycie danego urządzenia):



lub odwrotnie, z akcji „Dopuszcz” na akcję „Zablokuj”

Kolejność rozmieszczenia reguł ma znaczenie dla ich działania. Reguły są wykonywane od góry do dołu, czyli jeśli zadziała jakaś reguła, to następne w kolejności nie będą już dla niej stosowane. Kolejność zdefiniowanych reguł można zmieniać za pomocą strzałek ↑ i ↓ (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak ⊗ (również po prawej stronie).

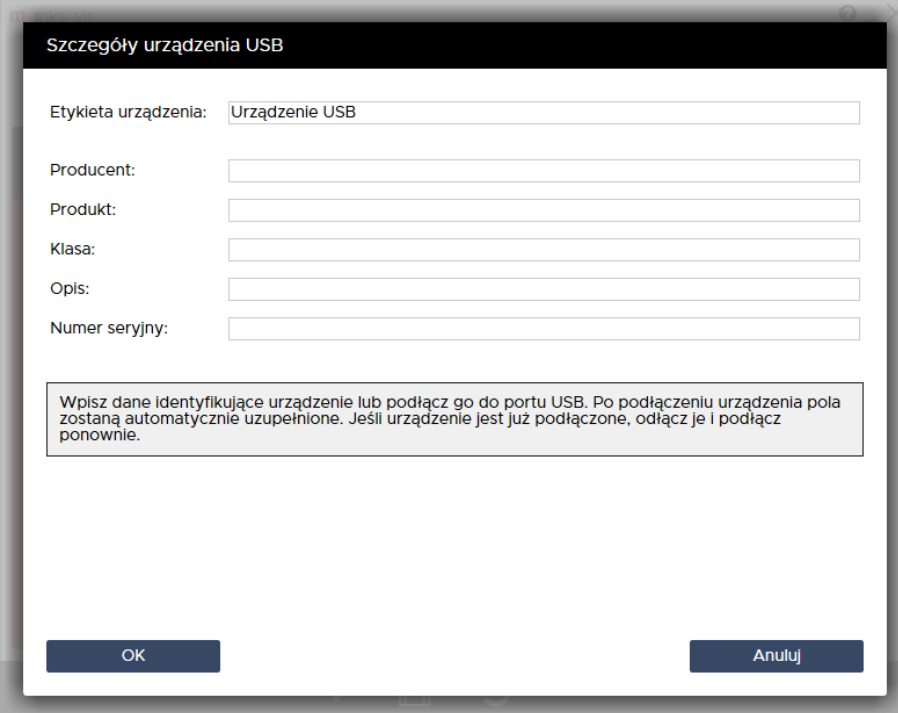
Po kliknięciu w opis urządzenia USB na liście reguł, otworzy się okno umożliwiające szczegółową modyfikację danej reguły:



Znak „=” na początku każdego pola reguły (oprócz pola „Etykieta urządzenia”, które jest tylko opisem nie mającym dla działania reguły żadnego znaczenia) powoduje, że zawartość danego

pola musi być identyczna z zawartością odpowiedniego pola podłączanego urządzenia, by reguła zadziałała

Wybranie „Dodaj urządzenie” spowoduje wyświetlenie pustego okna szczegółów urządzenia USB, co pozwala na ręczne lub półautomatyczne dodanie reguły (podłączenie do komputera nowego urządzenia USB w czasie wyświetlania tego okna spowoduje wypełnienie odpowiednich pól):



Szczegóły urządzenia USB

Etykieta urządzenia:

Producent:

Produkt:

Klasa:

Opis:

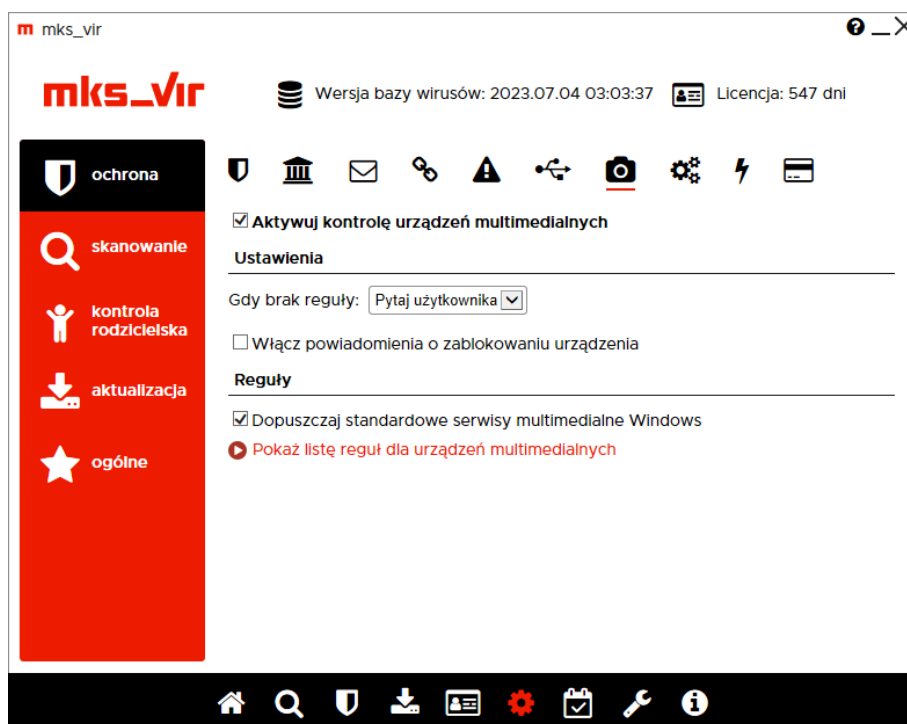
Numer seryjny:

Wpisz dane identyfikujące urządzenie lub podłącz go do portu USB. Po podłączeniu urządzenia pola zostaną automatycznie uzupełnione. Jeśli urządzenie jest już podłączone, odłącz je i podłącz ponownie.

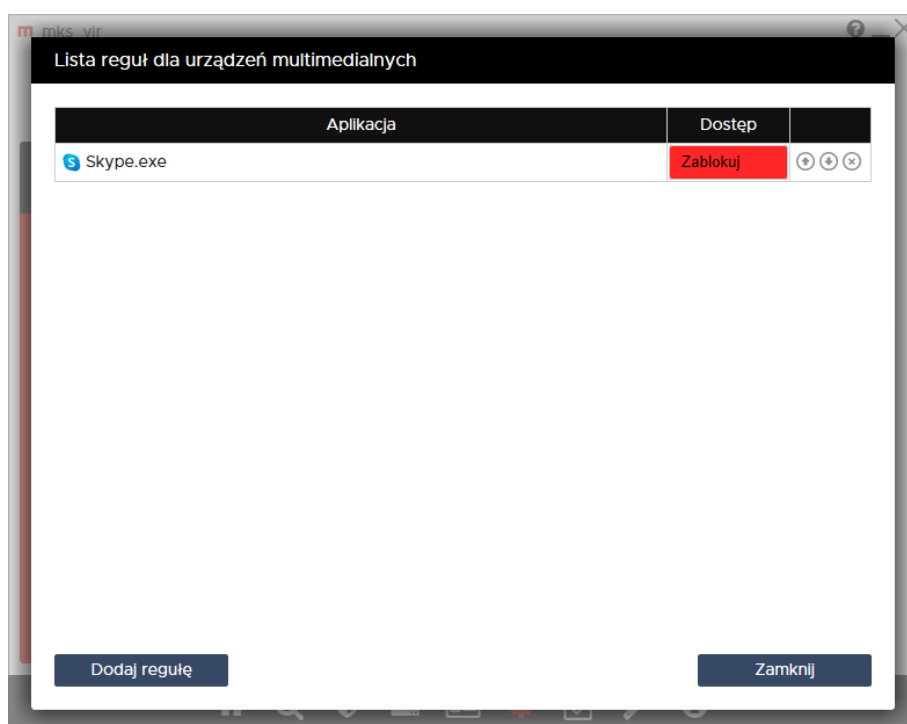
OK Anuluj

Jak zmodyfikować regułę w module „Kontrola urządzeń multimedialnych”

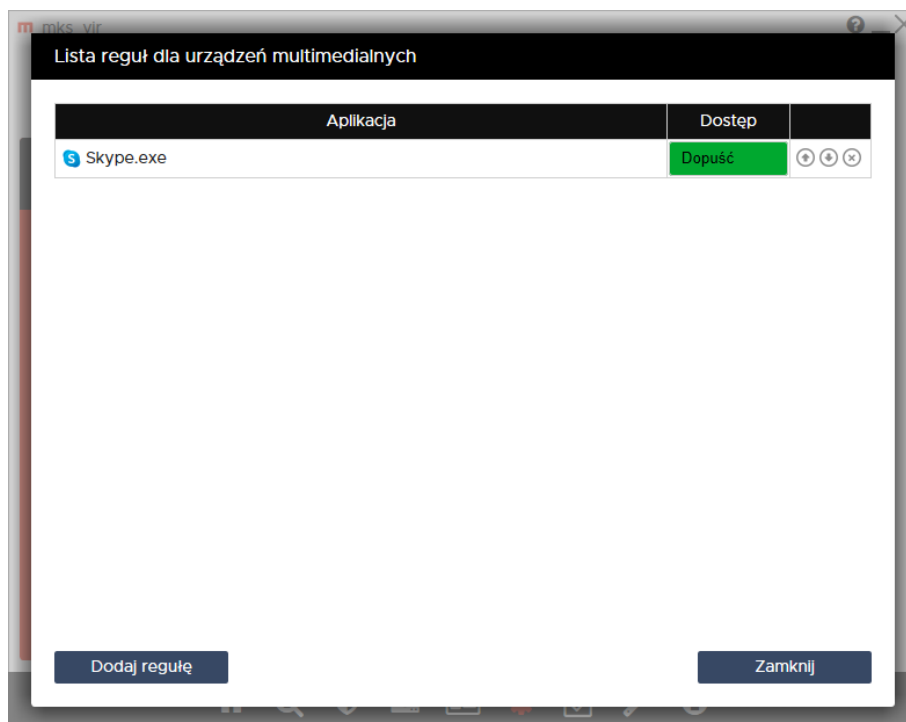
Aby zmodyfikować regułę utworzoną wcześniej w module „Kontrola urządzeń multimedialnych” programu **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do „Ochrona → Kontrola urządzeń multimedialnych → Pokaż listę reguł dla urządzeń multimedialnych”



Modyfikując utworzoną regułę przede wszystkim można zmienić tryb dostępu do urządzeń multimedialnych dla danej aplikacji, np. z akcji „Zablokuj” (czyli nie zezwalającej na dostęp):



na akcję „Dopusć” (czyli zezwalającą na dostęp):

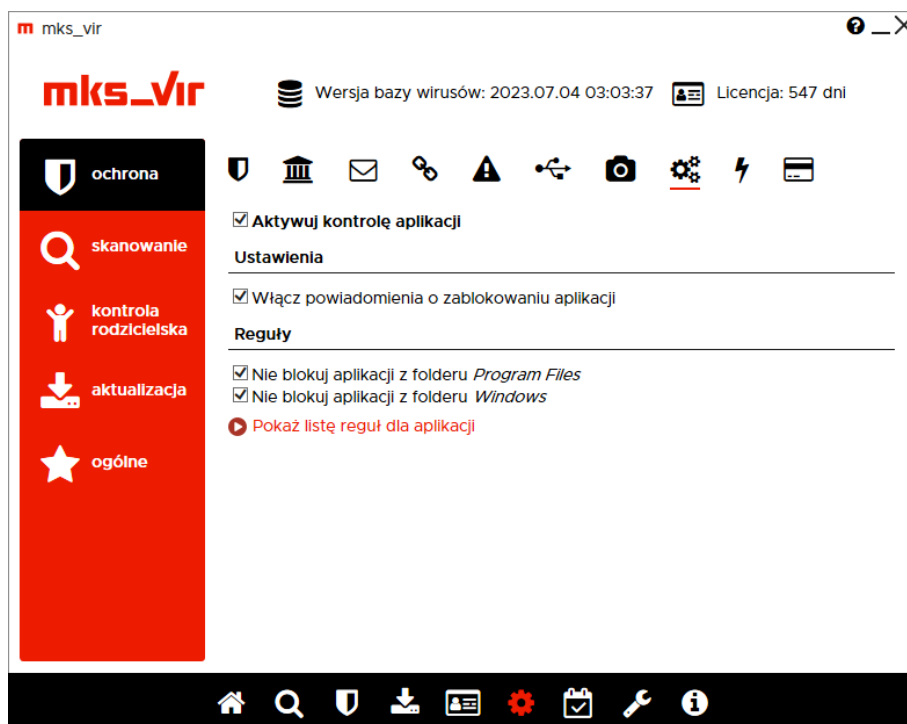


lub odwrotnie, z akcji „Dopusć” na akcję „Zablokuj”

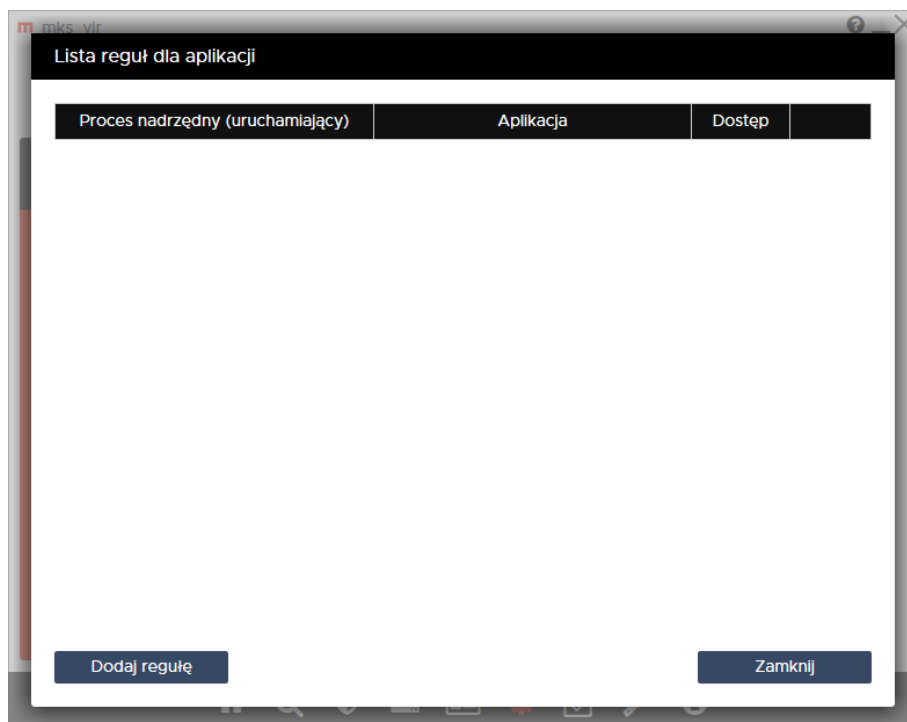
Kolejność rozmieszczenia reguł ma znaczenie dla ich działania. Reguły są wykonywane od góry do dołu, czyli jeśli zadziała jakaś reguła, to następne w kolejności nie będą już dla niej stosowane. Kolejność zdefiniowanych reguł można zmieniać za pomocą strzałek ↑ i ↓ (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak ⊗ (również po prawej stronie).

Jak utworzyć regułę w module „Kontrola aplikacji”

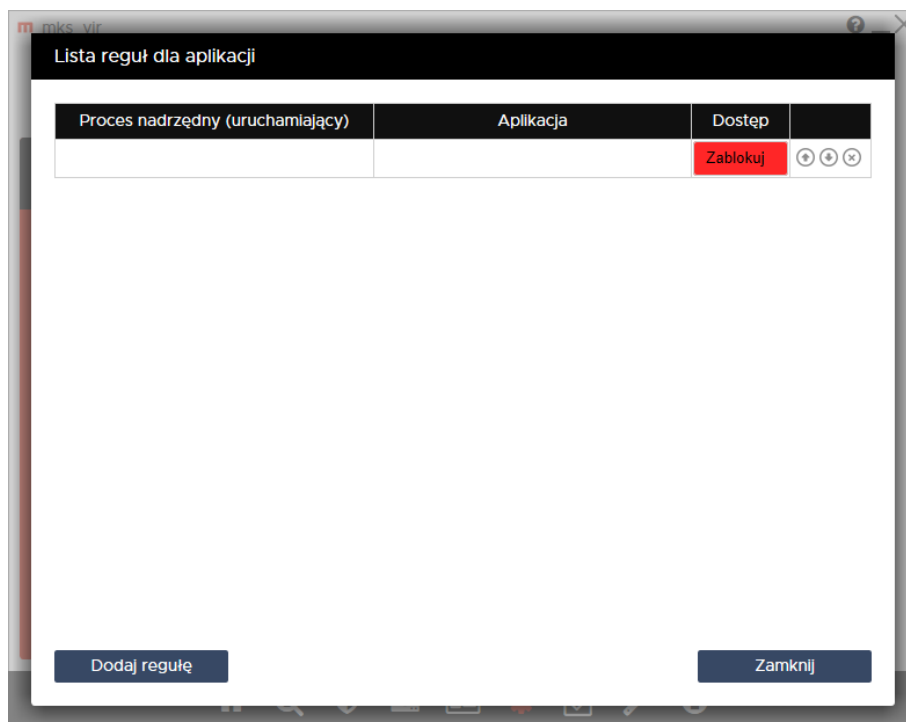
Aby utworzyć regułę w module „Kontrola aplikacji” programu **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do „Ochrona → Kontrola aplikacji → Pokaż listę reguł dla aplikacji”



Po otwarciu tej opcji pojawi się okno umożliwiające tworzenie własnych reguł lub modyfikowanie już istniejących:



Wybranie „Dodaj regułę” na dole okna powoduje dodanie edytowalnego wiersza, pozwalającego na zdefiniowanie własnej reguły (kolejne wybieranie „Dodaj regułę” będzie dodawało kolejne wiersze):



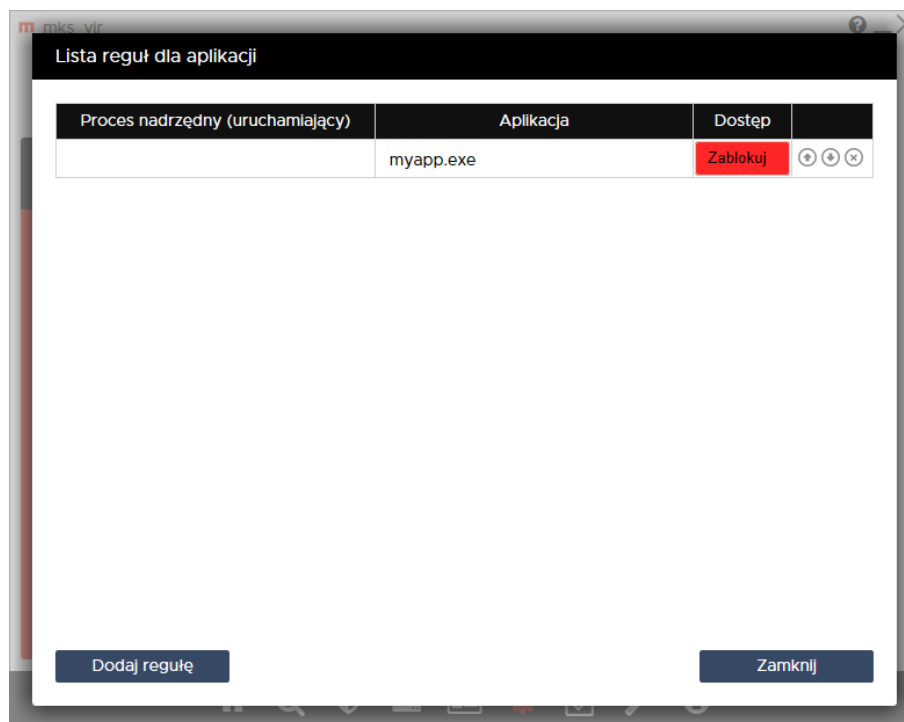
Poszczególne kolumny oznaczają:

- **Proces nadrzędny (uruchamiający)** – kolumna umożliwiająca zdefiniowanie reguły określającej aplikację, która sama będzie mogła być uruchamiana w każdym przypadku, ale albo nie będzie mogła („Zablokuj”), albo będzie mogła („Dopusć”), uruchamiać podrzędną aplikację zdefiniowaną w kolumnie „Aplikacja”
- **Aplikacja** – kolumna umożliwiająca zdefiniowanie reguły określającej aplikację, która ma być blokowana lub dopuszczana przy próbie uruchomienia
- **Dostęp** – kolumna określająca, czy dana aplikacja zdefiniowana przez regułę w kolumnie „Aplikacja” ma być blokowana przy próbie jej uruchomienia („Zablokuj”), czy też ma być zezwalane jej uruchamianie („Dopusć”)

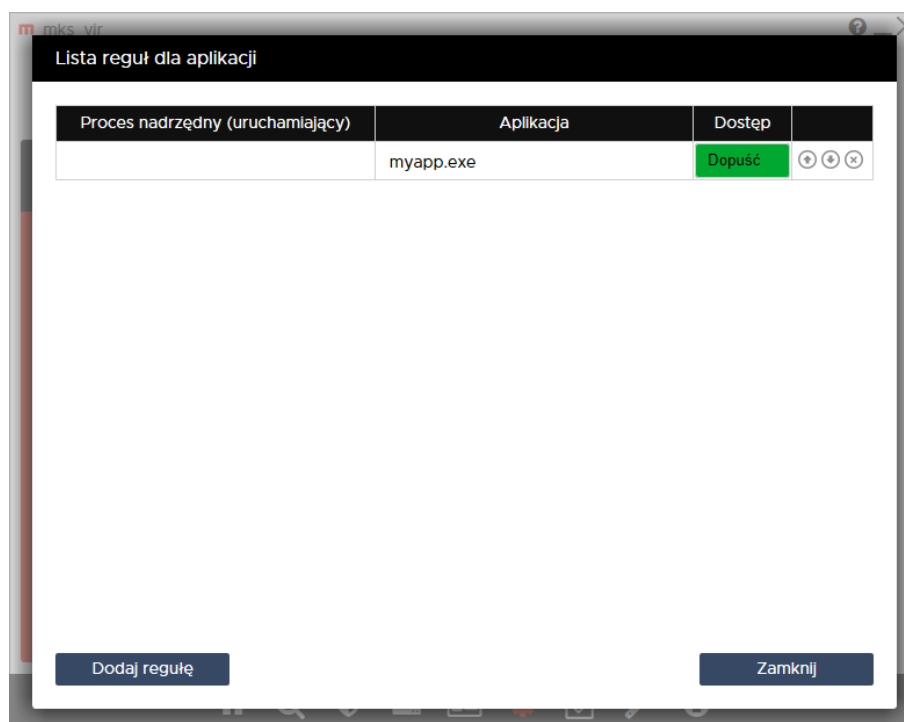
Należy mieć na uwadze, że w zależności od aktywności opcji „Nie blokuj aplikacji z folderu Program Files” i „Nie blokuj aplikacji z folderu Windows”, poszczególne reguły mogą działać lub nie, zależnie od lokalizacji aplikacji (czyli folderu, w którym aplikacja się znajduje), której dotyczy dana reguła

Przykładowe definicje reguł blokujących lub dopuszczających aplikacje:

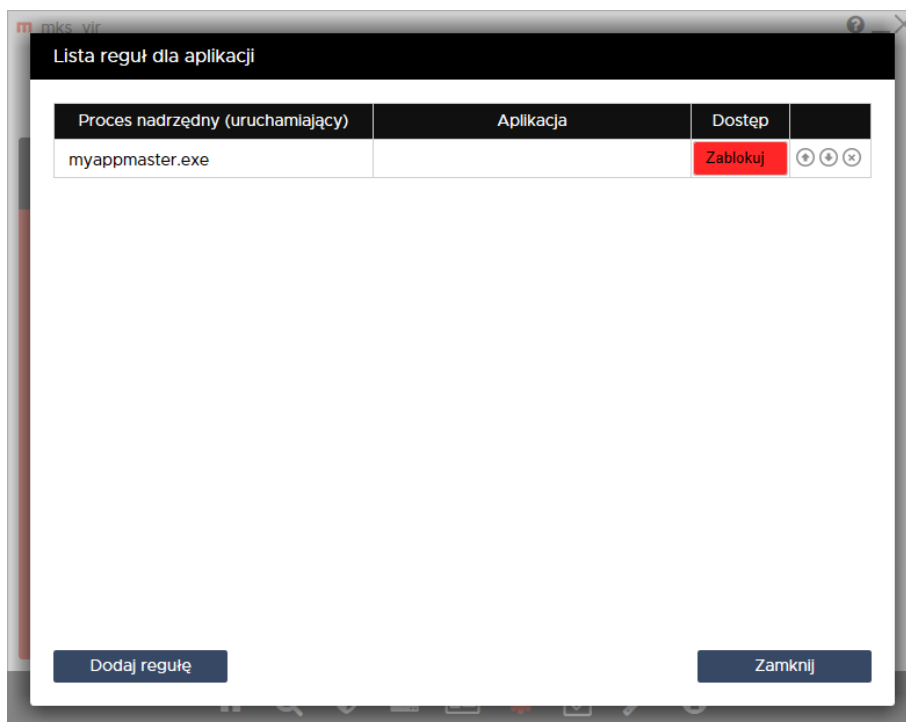
- definicja reguły blokującej próbę uruchomienia aplikacji (w przykładzie zdefiniowanej jako *myapp.exe*) w każdym przypadku:



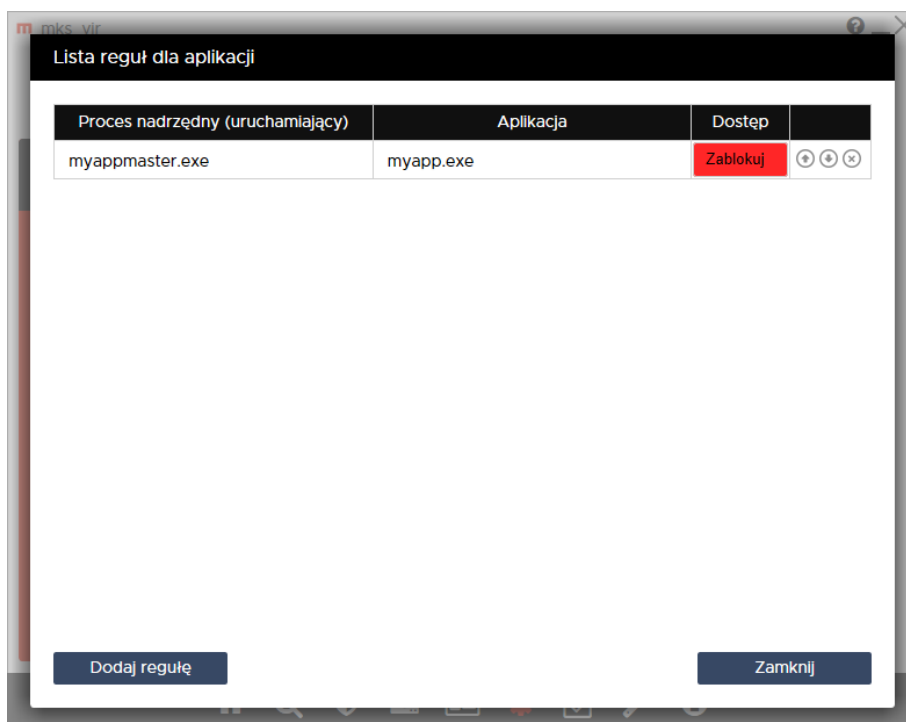
- definicja reguły dopuszczającej uruchamianie aplikacji (w przykładzie zdefiniowanej jako *myapp.exe*) w każdym przypadku:



- definicja reguły uniemożliwiającej uruchomienie dowolnego procesu podrzędnego (aplikacji) przez proces nadrzędny (tu zdefiniowanego jako *myappmaster.exe*):



- definicja reguły uniemożliwiającej uruchomienie procesu podrzędnego (aplikacji – tu zdefiniowanej jako *myapp.exe*) przez proces nadrzędny (tu zdefiniowanego jako *myappmaster.exe*), przy czym wszystkie inne procesy podrzędne są dopuszczane:

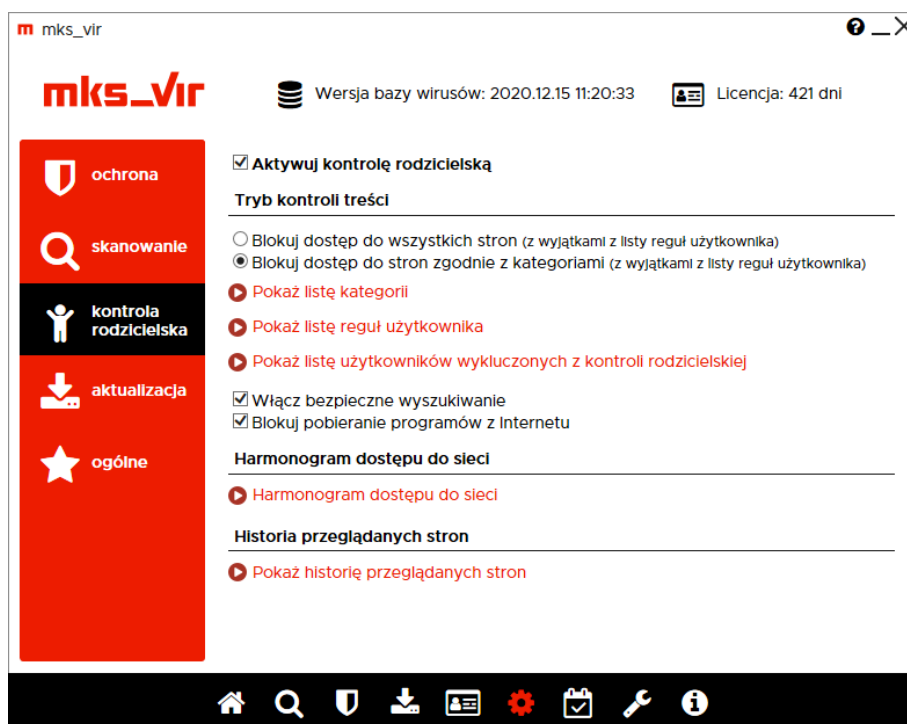


Kolejność rozmieszczenia reguł ma znaczenie dla ich działania. Reguły są wykonywane od góry do dołu, czyli jeśli zadziała jakaś reguła, to następne w kolejności nie będą już dla niej stosowane. Kolejność zdefiniowanych reguł można zmieniać za pomocą strzałek ⬆ i ⬇ (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak ⊗ (również po prawej stronie).

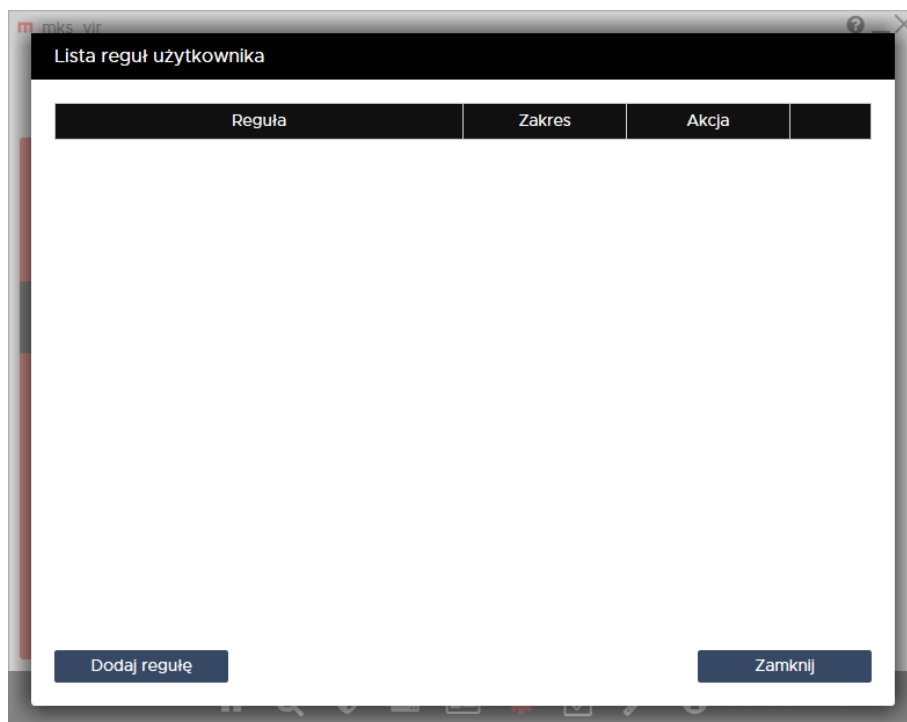
Jak utworzyć i zmodyfikować reguły użytkownika w module „Kontrola rodzicielska”

Uwaga! Aby tworzone lub modyfikowane reguły w module „Kontrola rodzicielska” działały, moduł ten należy uprzednio aktywować w programie **mks_vir**.

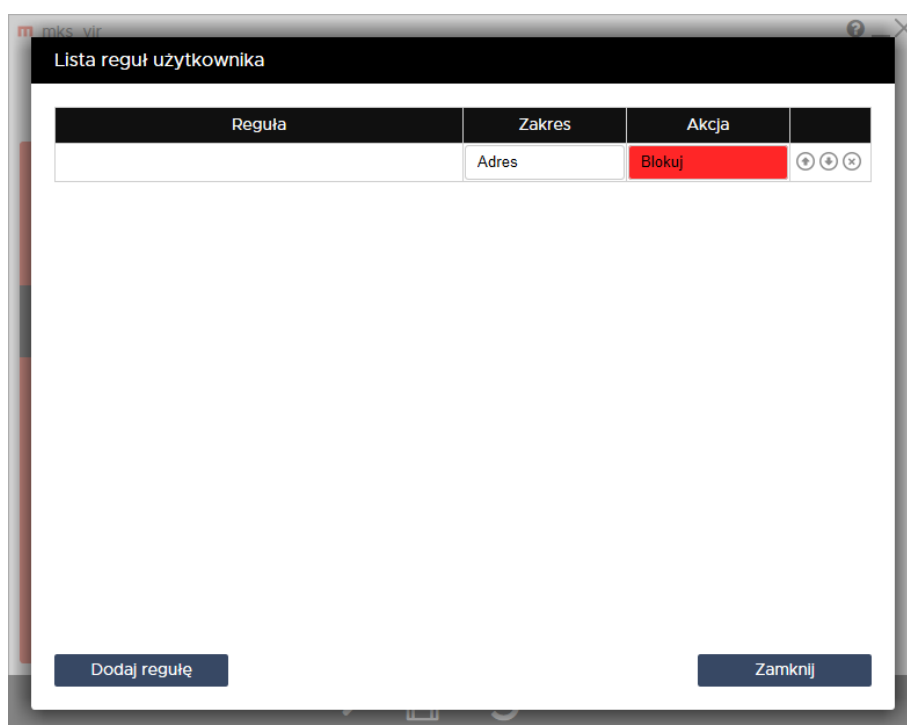
W module „Kontrola rodzicielska” jest możliwość definiowania własnych reguł filtrujących dla przeglądanych stron www. Aby utworzyć lub zmodyfikować własne reguły w tym module należy otworzyć główne okno programu **mks_vir**, wybrać „Ustawienia”, a następnie przejść do „Kontrola rodzicielska → Pokaż listę reguł użytkownika”:



Po otwarciu tej opcji pojawi się okno umożliwiające tworzenie własnych reguł lub modyfikowanie już istniejących:



Aby utworzyć własną regułę należy wybrać „Dodaj regułę”, pojawi się wtedy możliwość wpisania własnych definicji, dla których otwierane strony www mają być analizowane i zależnie od tego przepuszczane lub blokowane:



Definicje wpisujemy w polach kolumny „Reguła”, w kolumnie „Zakres” określamy obszar działania danej reguły:

- **Adres** – reguła będzie działała tylko w obszarze adresu otwieranej strony www
- **Treść** – reguła będzie działała tylko w obszarze zawartości otwieranej strony www

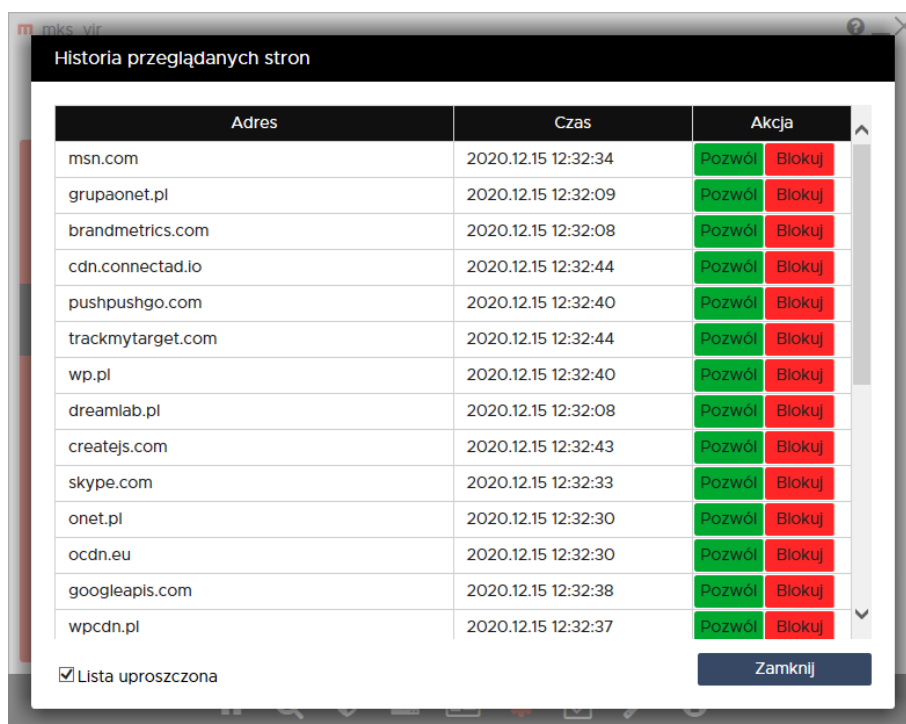
- **Wszędzie** – reguła będzie działała zarówno w obszarze adresu, jak i w obszarze zawartości otwieranej strony www

zaś w kolumnie „Akcja” określamy sposób działania danej reguły:

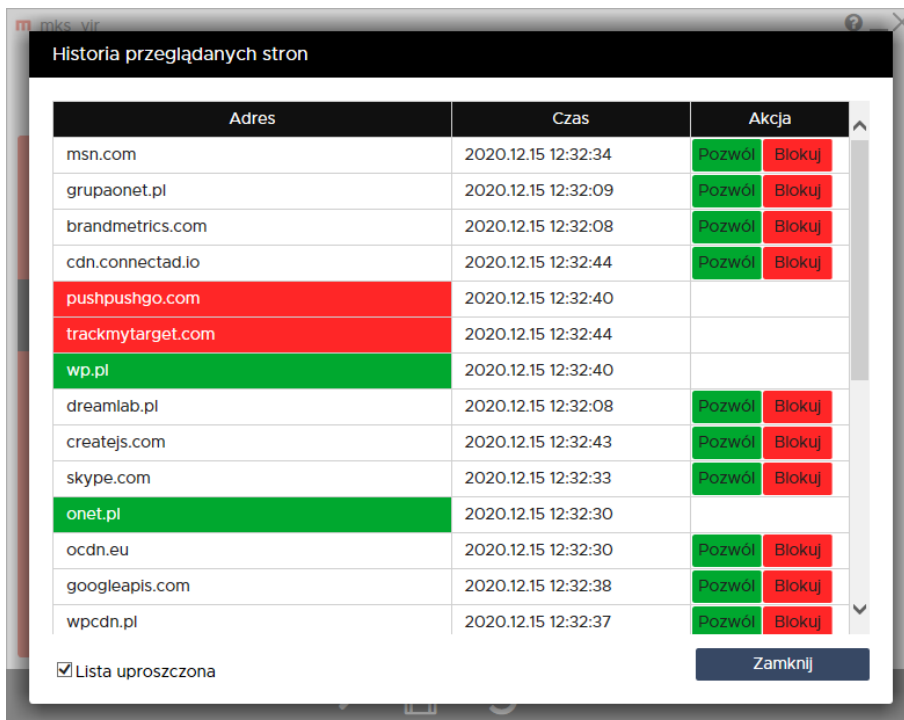
- **Blokuj** – zadziałanie reguły spowoduje zablokowanie otwieranej strony www
- **Pozwól** – zadziałanie reguły spowoduje przepuszczenie otwieranej strony www

Kolejność rozmieszczenia reguł ma znaczenie dla ich działania. Reguły są wykonywane od góry do dołu, czyli jeśli dla otwieranej strony www zadziała jakaś reguła, to następne w kolejności nie będą już dla niej stosowane. Kolejność zdefiniowanych reguł można zmieniać za pomocą strzałek ↑ i ↓ (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak ⊗ (również po prawej stronie).

Własne reguły można tworzyć także na podstawie historii przeglądanych stron www. W tym celu należy otworzyć główne okno programu **mks_vir**, wybrać „Ustawienia”, a następnie przejść do „Kontrola rodzicielska → Pokaż historię przeglądanych stron”:



Wybierając dla danej strony widocznej w kolumnie „Adres” odpowiednio „Pozwól” (jeśli strona ma być przepuszczana) lub „Blokuj” (jeśli strona ma być blokowana):

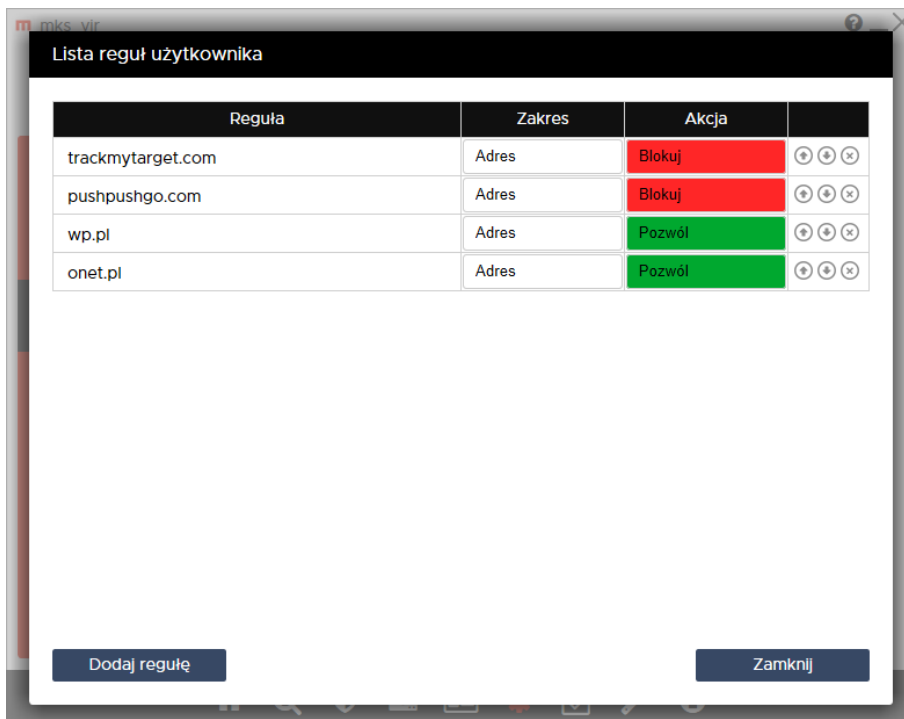


Adres	Czas	Akcja	
msn.com	2020.12.15 12:32:34	Pozwól	Blokuj
grupaonet.pl	2020.12.15 12:32:09	Pozwól	Blokuj
brandmetrics.com	2020.12.15 12:32:08	Pozwól	Blokuj
cdn.connectad.io	2020.12.15 12:32:44	Pozwól	Blokuj
pushpushgo.com	2020.12.15 12:32:40		
trackmytarget.com	2020.12.15 12:32:44		
wp.pl	2020.12.15 12:32:40		
dreamlab.pl	2020.12.15 12:32:08	Pozwól	Blokuj
createjs.com	2020.12.15 12:32:43	Pozwól	Blokuj
skype.com	2020.12.15 12:32:33	Pozwól	Blokuj
onet.pl	2020.12.15 12:32:30		
ocdn.eu	2020.12.15 12:32:30	Pozwól	Blokuj
googleapis.com	2020.12.15 12:32:38	Pozwól	Blokuj
wpcdn.pl	2020.12.15 12:32:37	Pozwól	Blokuj

Lista uproszczona

Zamknij

Tak zmodyfikowane wiersze historii automatycznie tworzą odpowiednie reguły, które można sprawdzić w „Pokaż listę reguł użytkownika”, a także ustalić dla nich odpowiednią kolejność:



Reguła	Zakres	Akcja	
trackmytarget.com	Adres	Blokuj	⊕ ⊖ ⊗
pushpushgo.com	Adres	Blokuj	⊕ ⊖ ⊗
wp.pl	Adres	Pozwól	⊕ ⊖ ⊗
onet.pl	Adres	Pozwól	⊕ ⊖ ⊗

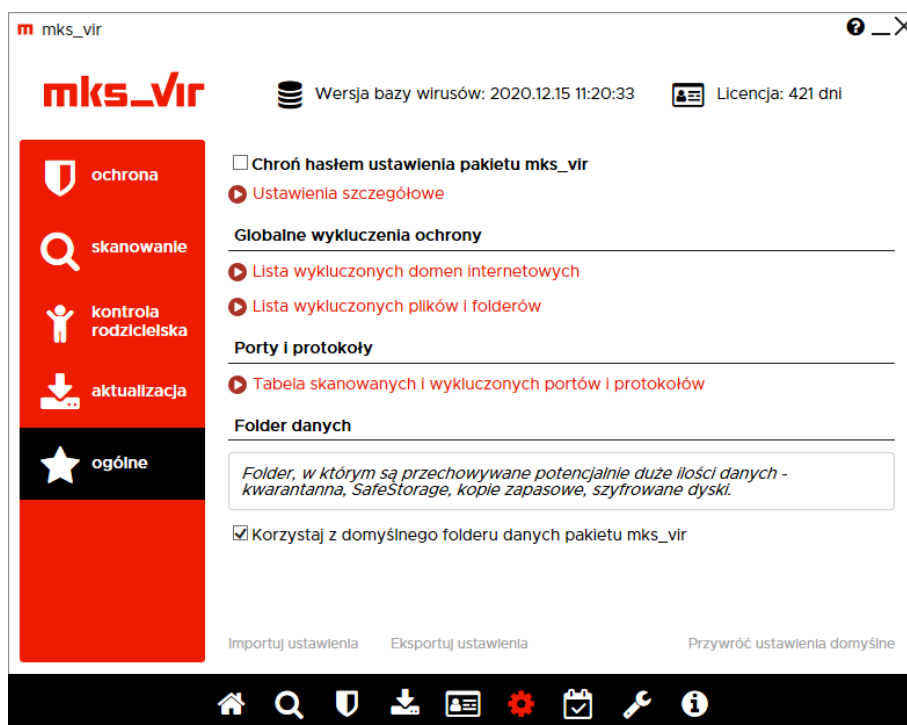
Dodaj regułę

Zamknij

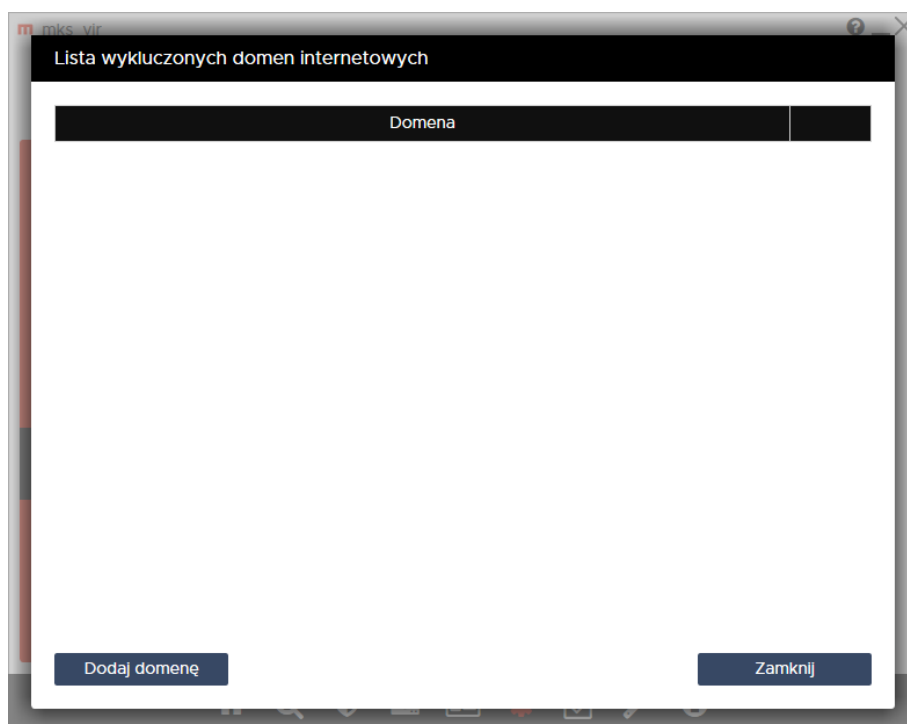
Jak dodać domenę internetową do wykluczeń

Instrukcja ta umożliwi zdefiniowanie adresów internetowych, dla których nie będą działały moduły ochrony przeglądarki i kontroli rodzicielskiej programu **mks_vir**

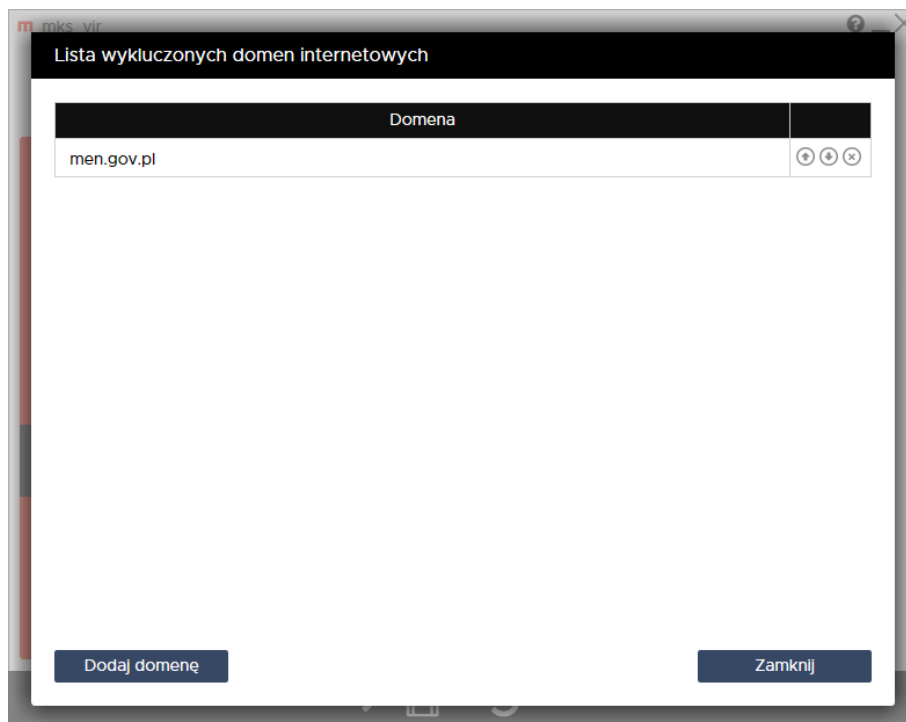
Aby dodać domenę internetową do wykluczeń w programie **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do sekcji „Ogólne”:



Po wybraniu „Lista wykluczonych domen internetowych” pojawi się okno z możliwością dodania domeny do wykluczeń:



Po wybraniu „Dodaj domenę” wpisujemy domenę, którą chcemy wykluczyć (w przykładzie wykluczona zostaje domena „https://men.gov.pl/”), po czym zamykamy okno „Listy wykluczonych domen internetowych” za pomocą przycisku „Zamknij”:

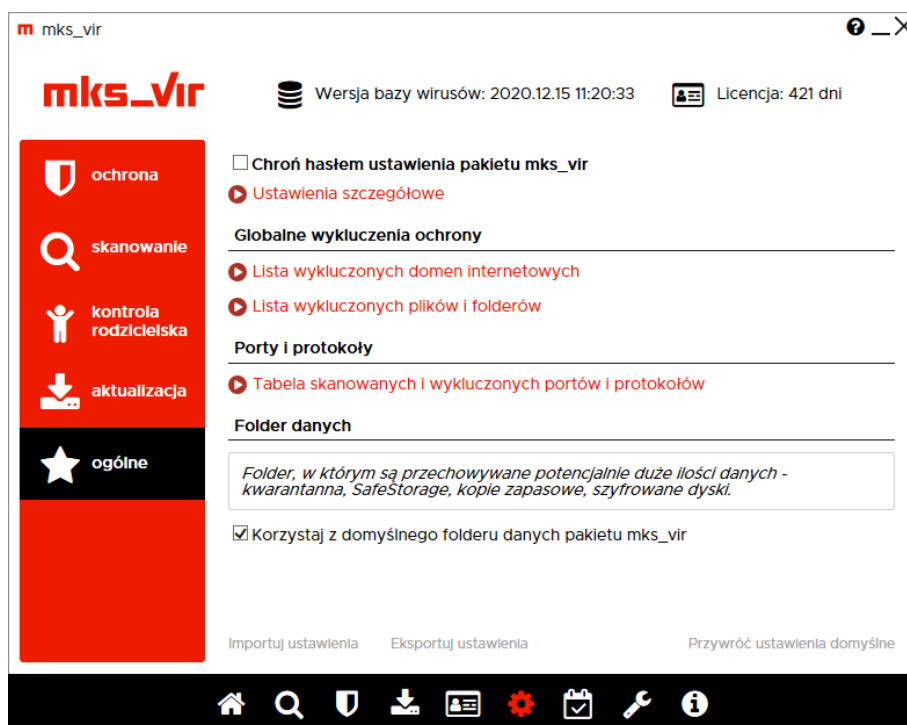


UWAGA! Aby reguły wykluczające działały poprawnie, należy dodawać same domeny, bez przedrostków „http://” czy „https://”, bez początkowego „www”, a także bez znaku ukośnika „/” po domenie i bez reszty elementów adresu internetowego.

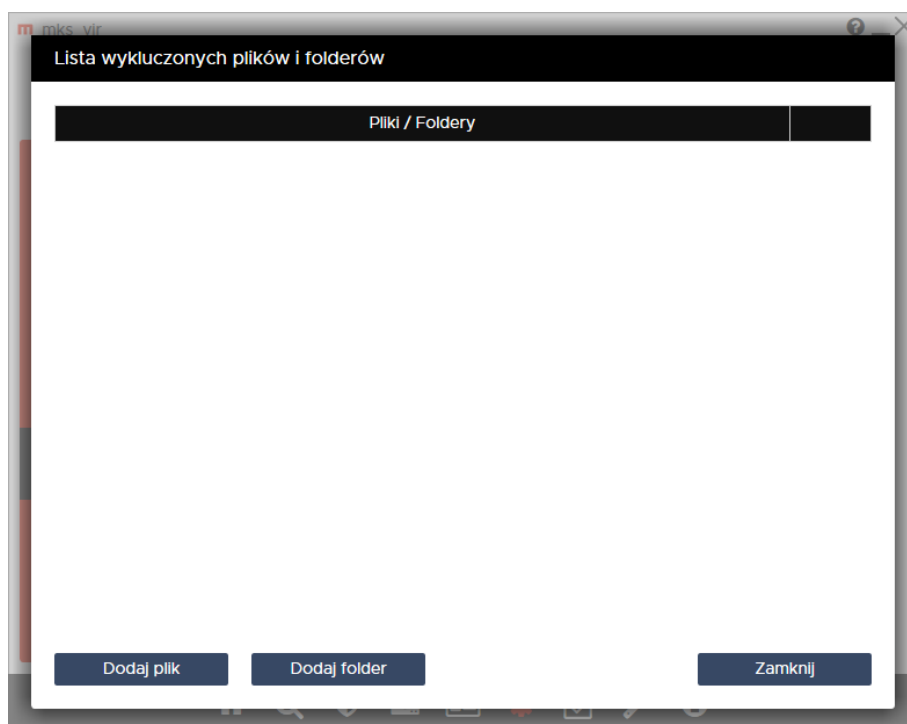
Jak dodać plik lub folder do wykluczeń

Instrukcja ta umożliwi zdefiniowanie obiektów (plików lub folderów), dla których nie będzie działał moduł ochrony plików programu **mks_vir**

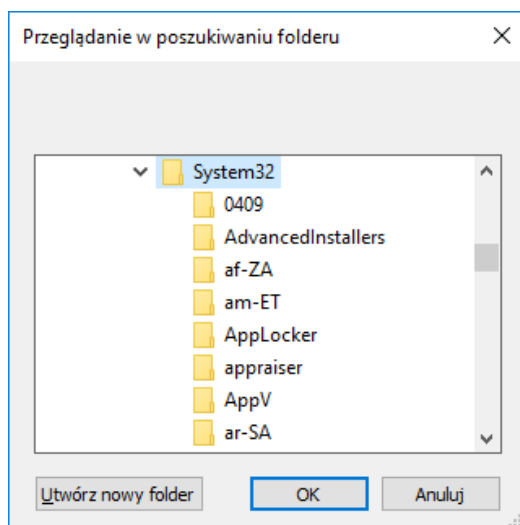
Aby dodać plik lub folder do wykluczeń w programie **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do sekcji „Ogólne”:



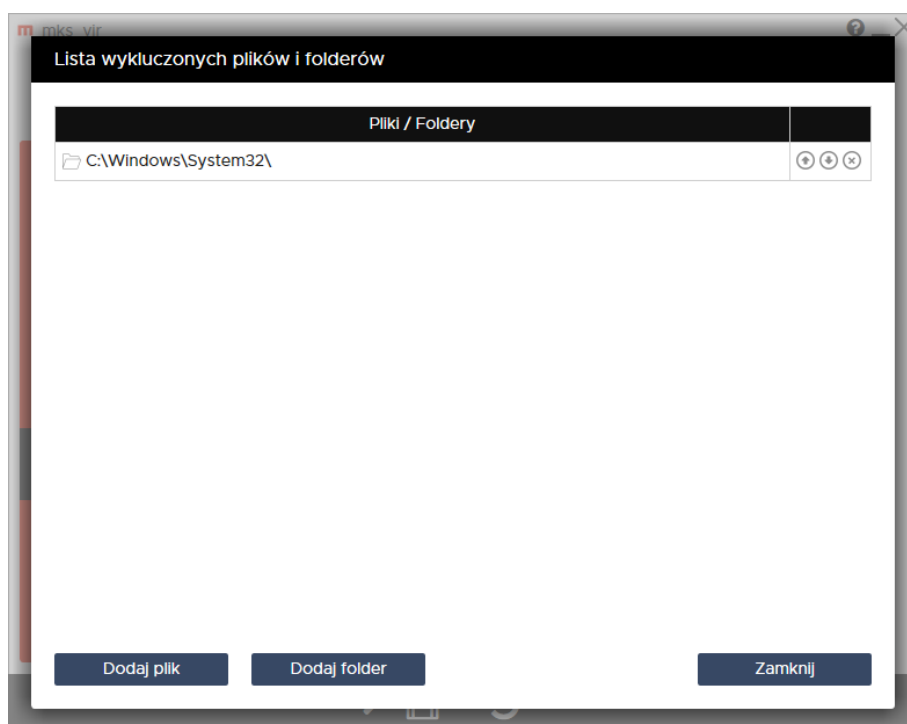
Po wybraniu „Lista wykluczonych plików i folderów” pojawi się okno z możliwością dodania pliku lub folderu do wykluczeń:



Po wybraniu „Dodaj plik” lub „Dodaj folder”, zależnie od tego czy chcemy wykluczyć plik czy folder. Z listy wybieramy co chcemy wykluczyć zaznaczając to (w przykładzie wykluczony jest folder) i klikając „OK”:



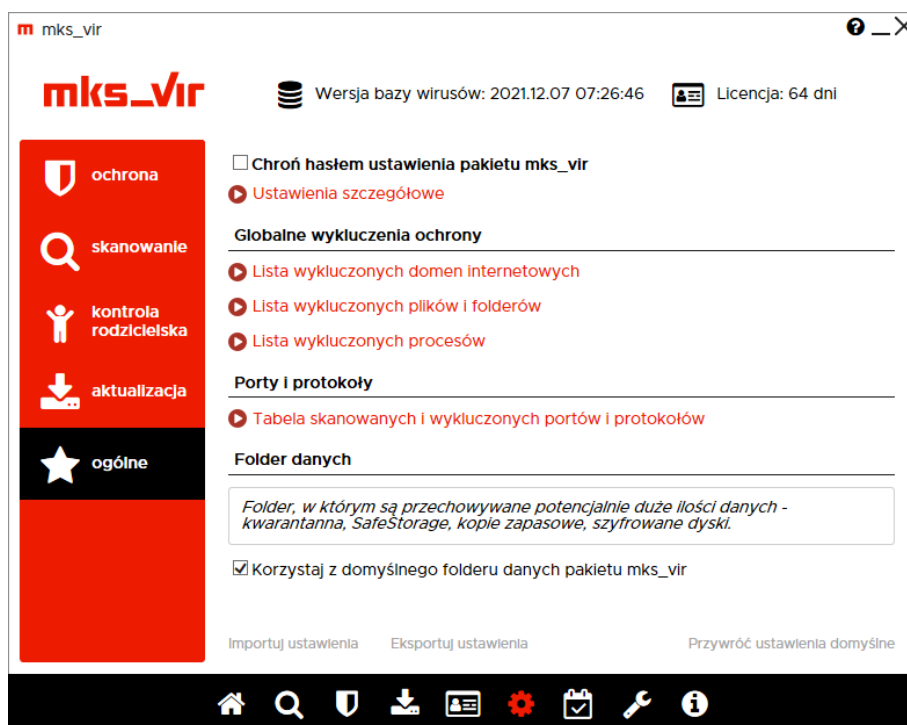
Na koniec zamykamy okno „Listy wykluczonych plików i folderów” za pomocą przycisku „Zamknij”:



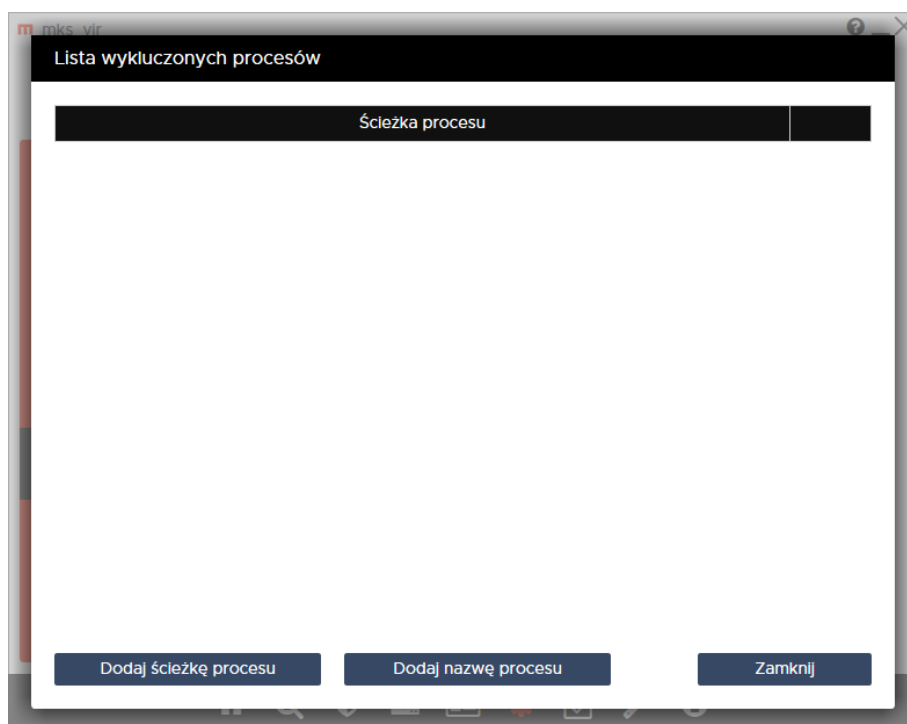
Jak dodać proces do wykluczeń

Instrukcja ta umożliwi zdefiniowanie procesów (programów), dla których nie będzie działał moduł ochrony plików programu **mks_vir**

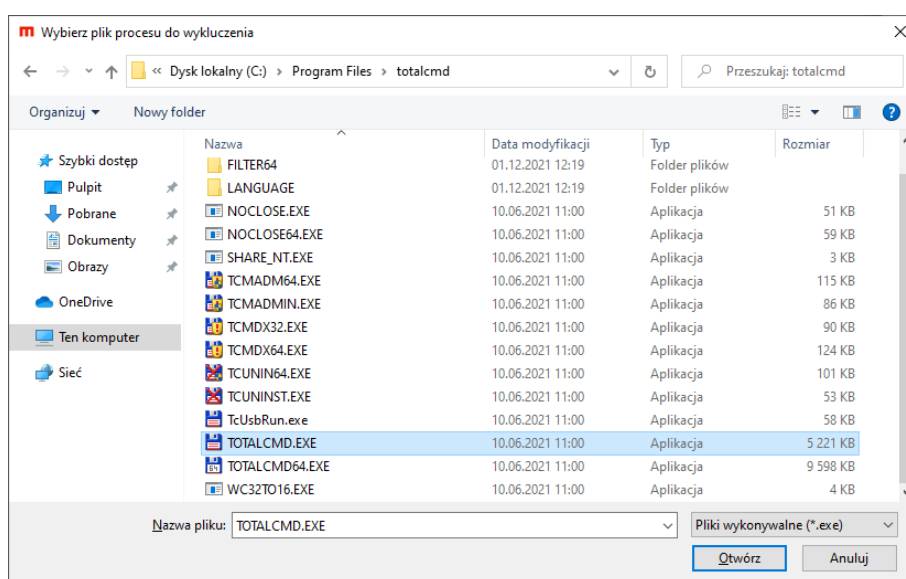
Aby dodać proces do wykluczeń w programie **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do sekcji „Ogólne”:



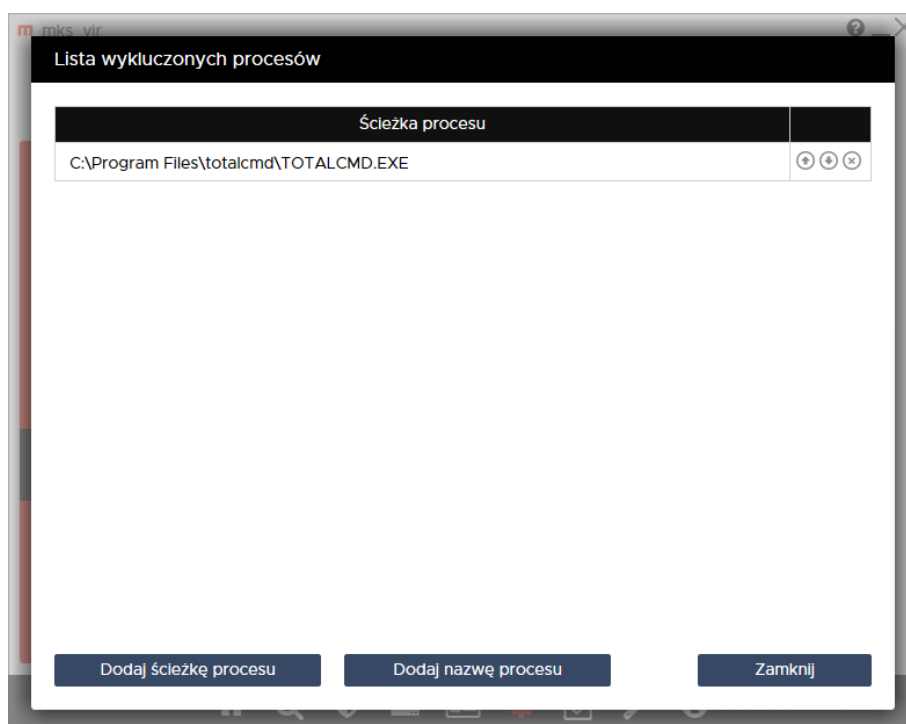
Po wybraniu „Lista wykluczonych procesów” pojawi się okno z możliwością dodania procesu (programu) do wykluczeń:



Po wybraniu „Dodaj ścieżkę procesu” z listy wybieramy program, który chcemy wykluczyć zaznaczając go (w przykładzie wykluczany jest „TOTALCMD.EXE”) i klikając „OK”:



Na koniec zamykamy okno „Listy wykluczonych procesów” za pomocą przycisku „Zamknij”:

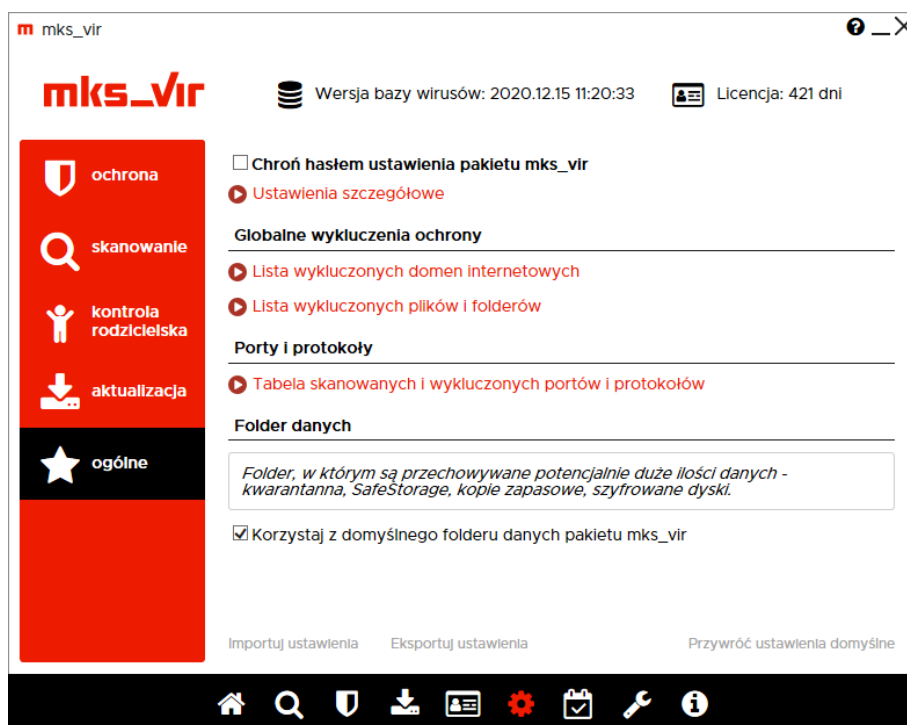


Po wybraniu „Dodaj nazwę procesu” można zdefiniować maskę definiującą wykluczane procesy, przy czym maska jest fragmentem ścieżki lub nazwy pliku (przykładowo proces „TOTALCMD.EXE” można wykluczyć z uwzględnieniem folderu instalacyjnego za pomocą maski „totalcmd\TOTALCMD.EXE”)

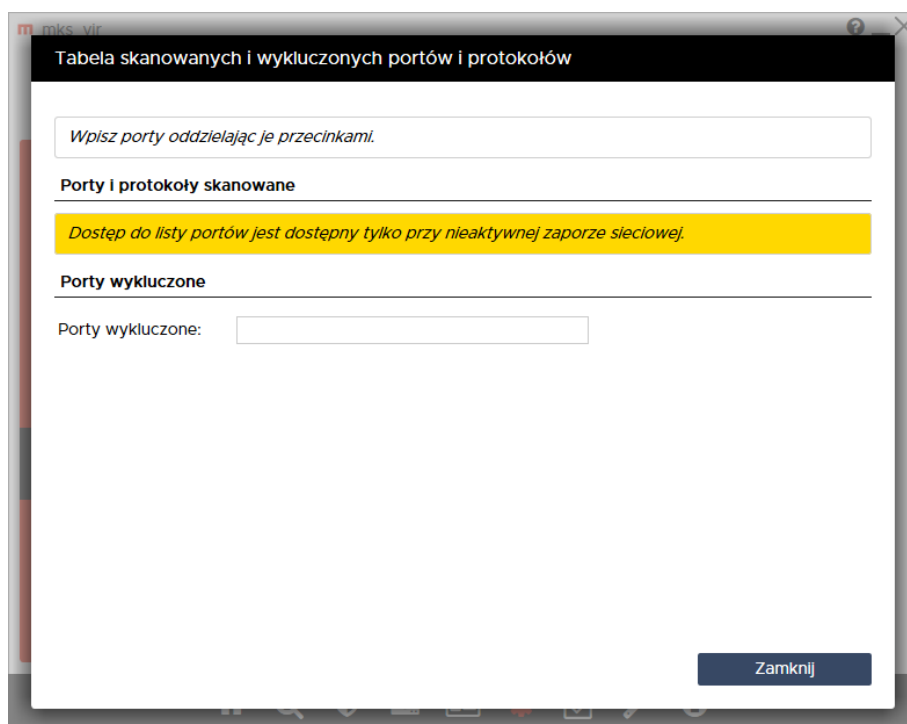
Jak dodać porty do wykluczeń

Instrukcja ta umożliwi zdefiniowanie portów, które mają być w ogóle wyłączone spod kontroli w programie **mks_vir**

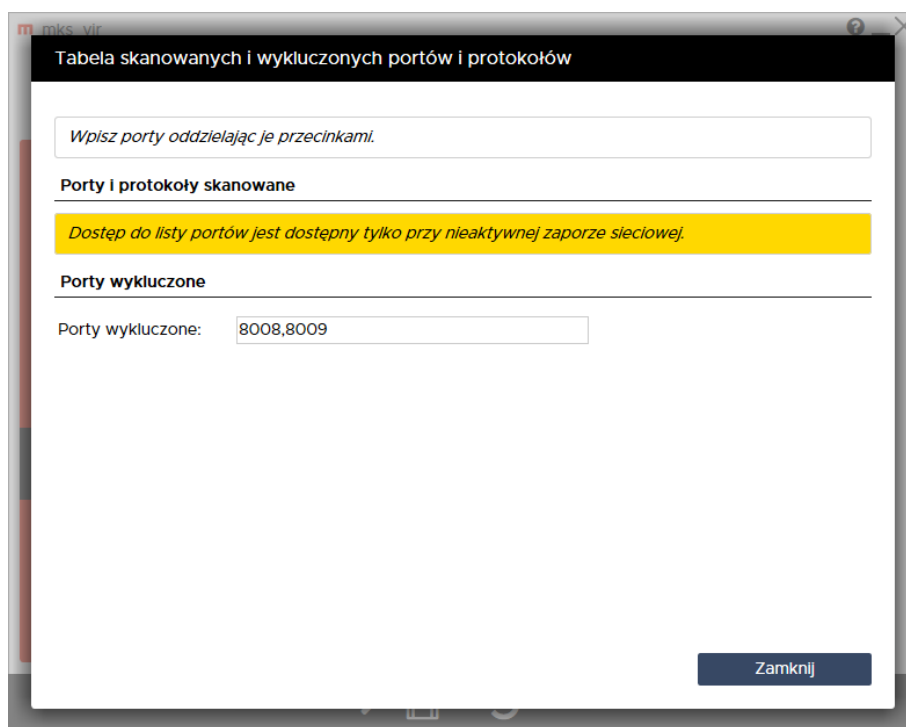
Aby dodać porty do wykluczeń w programie **mks_vir** należy otworzyć główne okno programu, wybrać „Ustawienia”, a następnie przejść do sekcji „Ogólne”:



Po wybraniu „Tabela skanowanych i wykluczonych portów i protokołów” pojawi się okno z możliwością dodania portów do wykluczeń:



Następnie wpisujemy port lub porty, jakie chcemy wykluczyć, w wierszu „Porty wykluczone” (w przykładzie wykluczone zostały dwa porty komunikacyjne wykorzystywane przez urządzenie „Chromecast”); przy wykluczaniu więcej niż jednego portu ich numery rozdzielamy przecinkami:

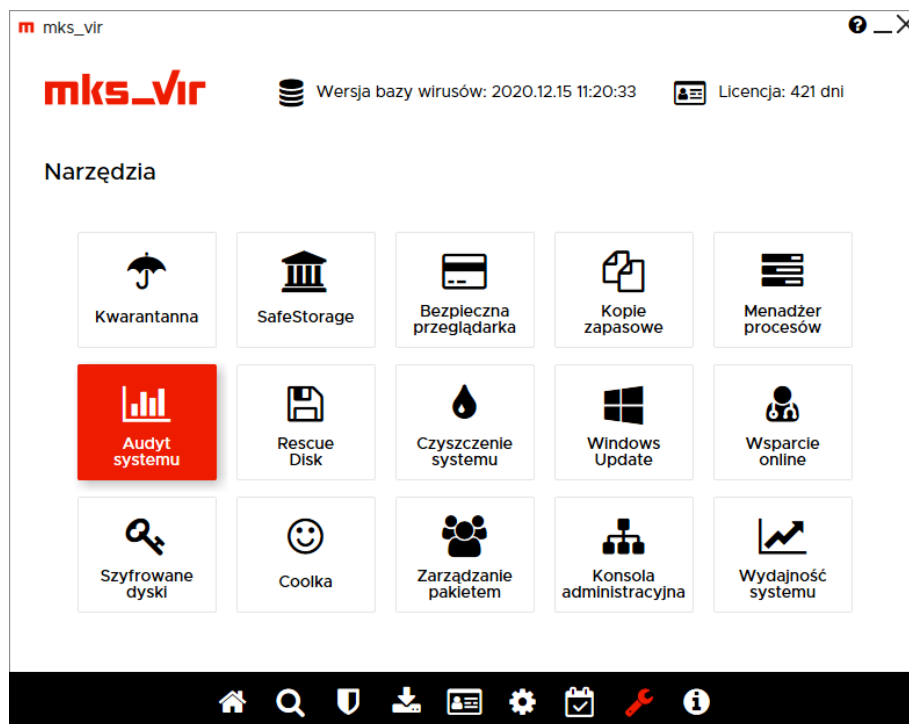


Po wpisaniu portów zamykamy okno „Tabeli skanowanych i wykluczonych portów i protokołów” za pomocą przycisku „Zamknij”

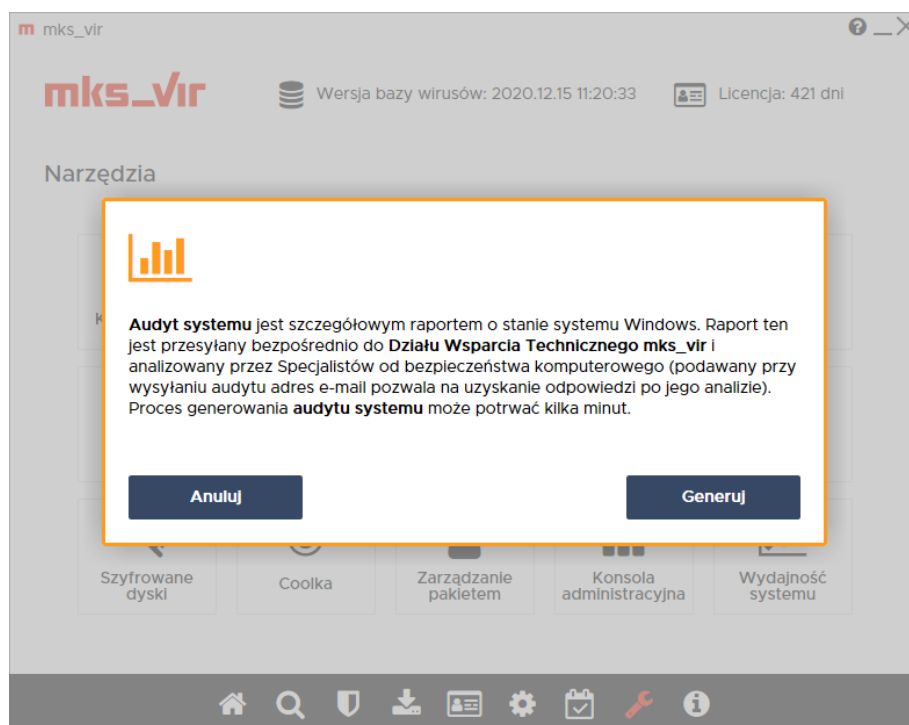
Jak utworzyć i wysłać audyt systemu

Aby utworzyć i wysłać audyt systemu programu **mks_vir** należy posłużyć się poniższą instrukcją:

1. uruchamiamy program **mks_vir** i przechodzimy do sekcji „Narzędzia”:

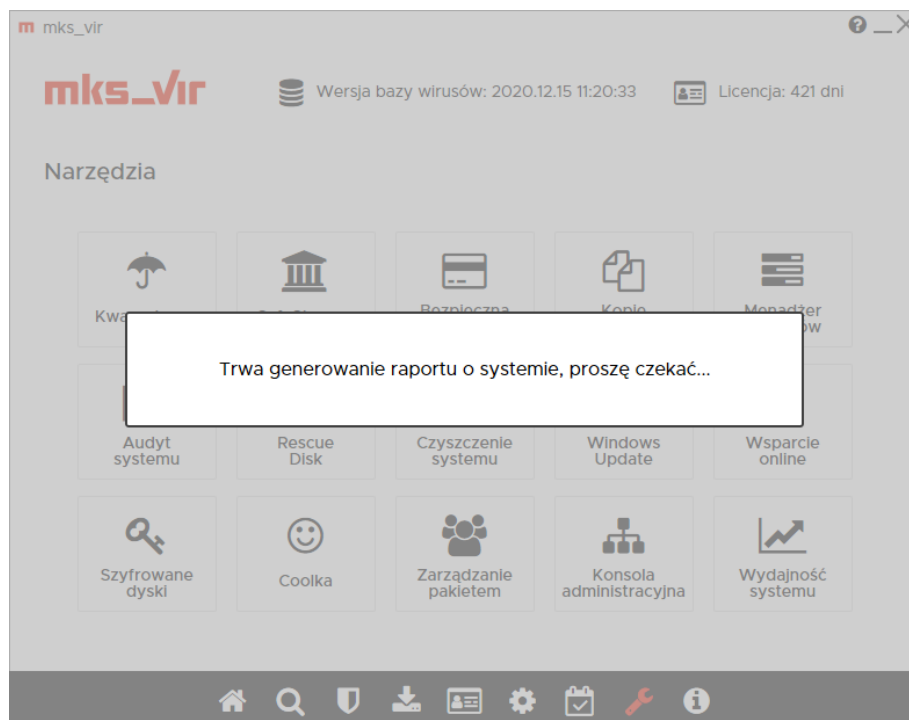


2. wybieramy „Audyt systemu”:



i klikamy „Generuj”

3. czekamy aż zakończy działanie:



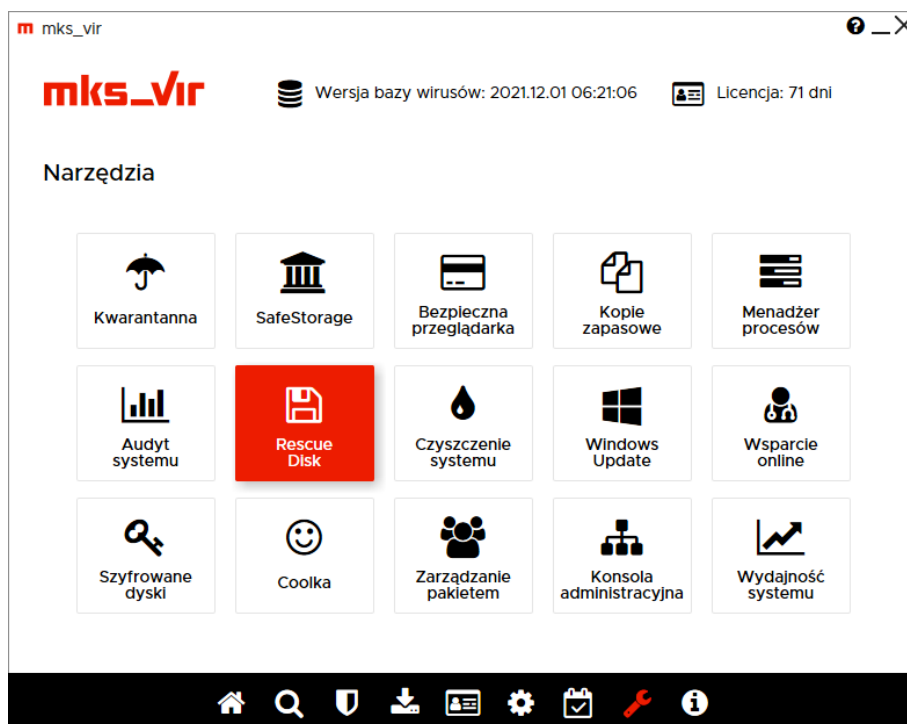
4. po zakończeniu generowania audytu systemu pojawi się formularz do wysłania go; wypełniamy wszystkie trzy pola wpisując:

- w pole „e-mail kontaktowy” swój adres email
- w pole „temat wiadomości” wpisując temat (ew. pozostawiając domyślny)
- w polu „wiadomość/opis problemu” opisując pokrótce problem

po czym wybieramy „Wyślij pliki”

Jak utworzyć nośnik ratunkowy „Rescue Disk”

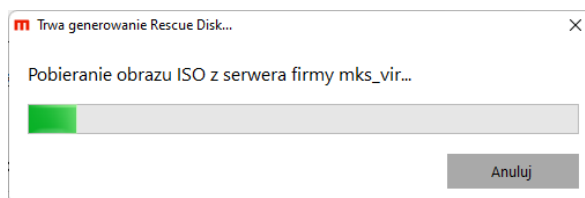
Aby utworzyć nośnik ratunkowy „Rescue Disk” w programie **mks_vir** należy najpierw włożyć do nagrywarki CD/DVD czystą płytę lub podłączyć czysty nośnik USB o pojemności nie większej niż 16 GB, na którym utworzymy nośnik ratunkowy (w instrukcji zostanie użyty nośnik USB). Następnie w głównym oknie programu **mks_vir** należy wybrać „Narzędzia”, po czym kliknąć w „Rescue Disk”:



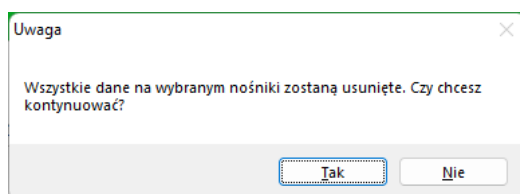
Po uruchomieniu narzędzia do tworzenia nośnika ratunkowego pojawi się okno:



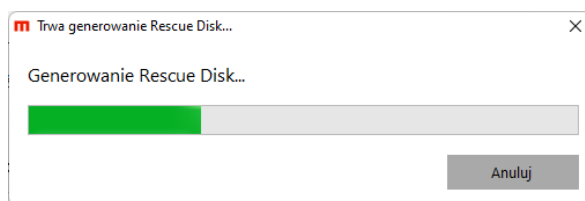
Pozostawiamy zaznaczoną opcję „Pobierz aktualny obraz ISO z serwera firmy mks_vir”, niżej wybieramy odpowiedni nośnik docelowy, po czym wciskamy „Generuj Rescue Disk”, co rozpocznie pobieranie aktualnego obrazu nośnika ratunkowego:



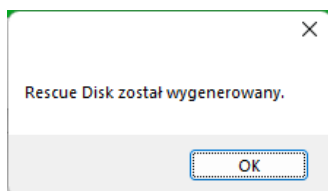
Gdy pobieranie się zakończy, pojawi się komunikat ostrzegający o całkowitej utracie znajdujących się ew. na nośniku danych:



Po kliknięciu „Tak” rozpocznie się właściwe tworzenie nośnika ratunkowego:



Gdy tworzenie zakończy się, pojawi się stosowny komunikat informujący, że nośnik ratunkowy „Rescue Disk” jest gotowy:



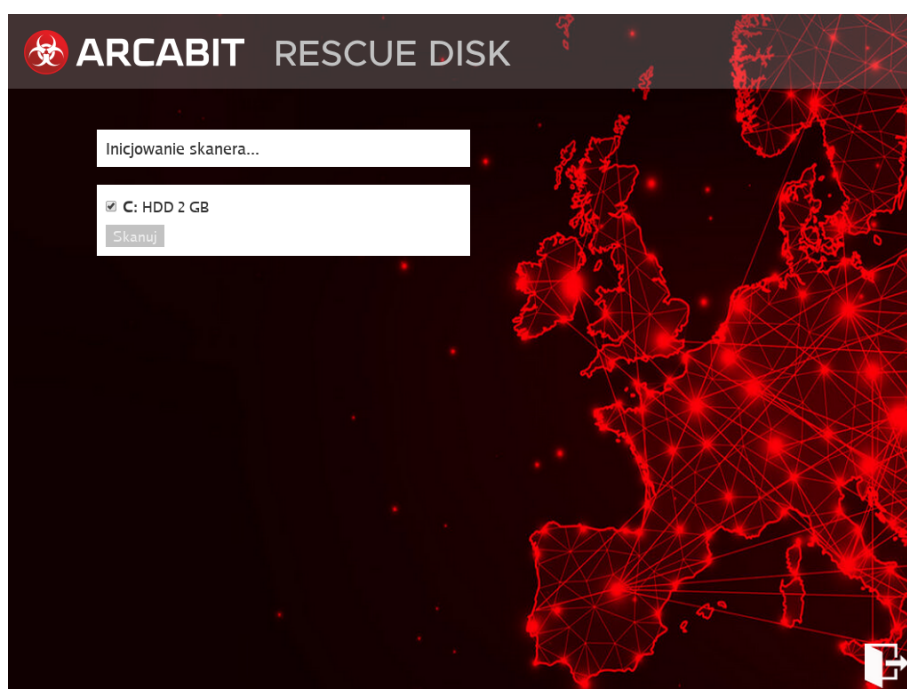
Korzystanie z nośnika ratunkowego „Rescue Disk”

Aby wykorzystać nośnik ratunkowy „Rescue Disk” należy po jego utworzeniu w programie **mks_vir** uruchomić za jego pomocą komputer (realizacja takiego uruchomienia komputera jest zależna od tego, czy nośnik ratunkowy został wykonany na płycie CD/DVD, czy na nośniku USB, a także od metod startu systemu ustawianego w BIOS komputera).

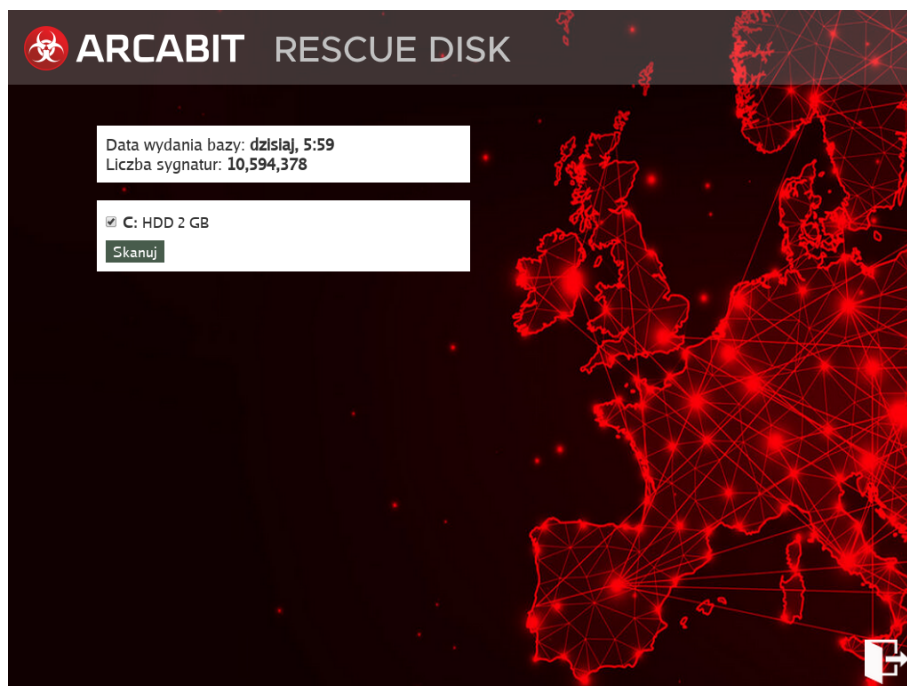
Po uruchomieniu komputera z nośnika ratunkowego „Rescue Disk” należy zgodzić się na warunki licencji, w przeciwnym razie narzędzie nie zostanie poprawnie zainicjowane:



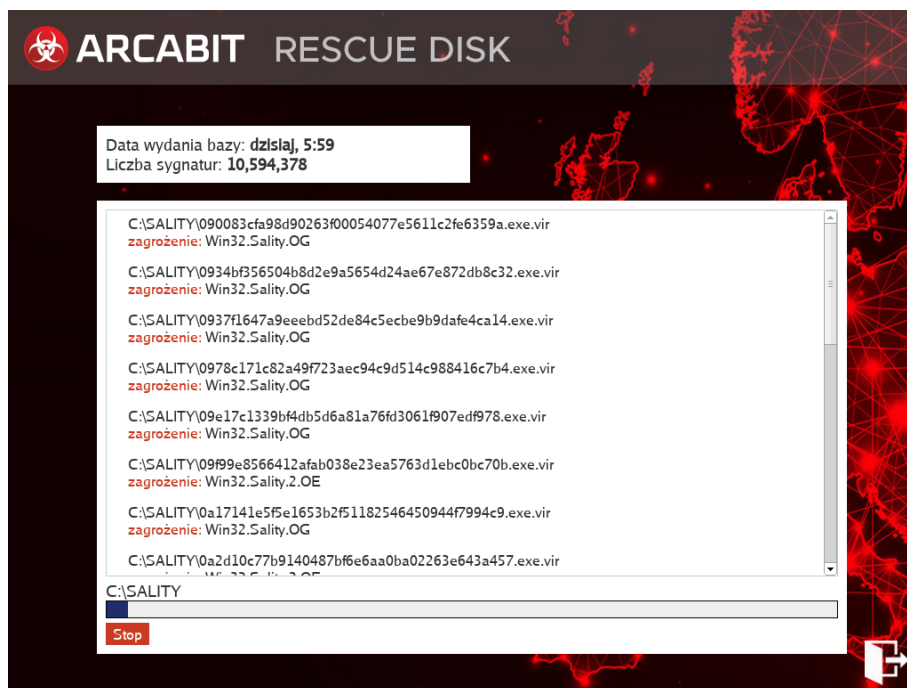
Po wyrażeniu zgody na warunki licencji, rozpocznie się inicjowanie silników skanujących (może to trochę potrwać i zależy jest od tego, czy „Rescue Disk” został uruchomiony z płyty CD/DVD, czy z nośnika USB, a także od wydajności procesora i ilości dostępnej pamięci RAM):



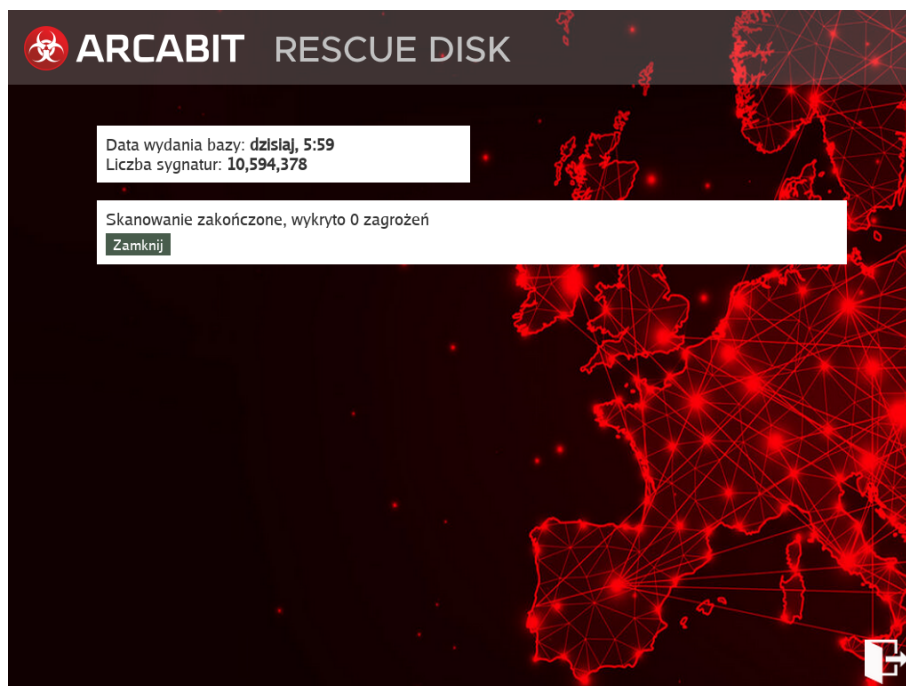
Po zainicjowaniu silników skanujących pojawi się informacja na temat bazy wirusów dostępnej w „Rescue Disk” oraz lista dostępnych do skanowania dysków:



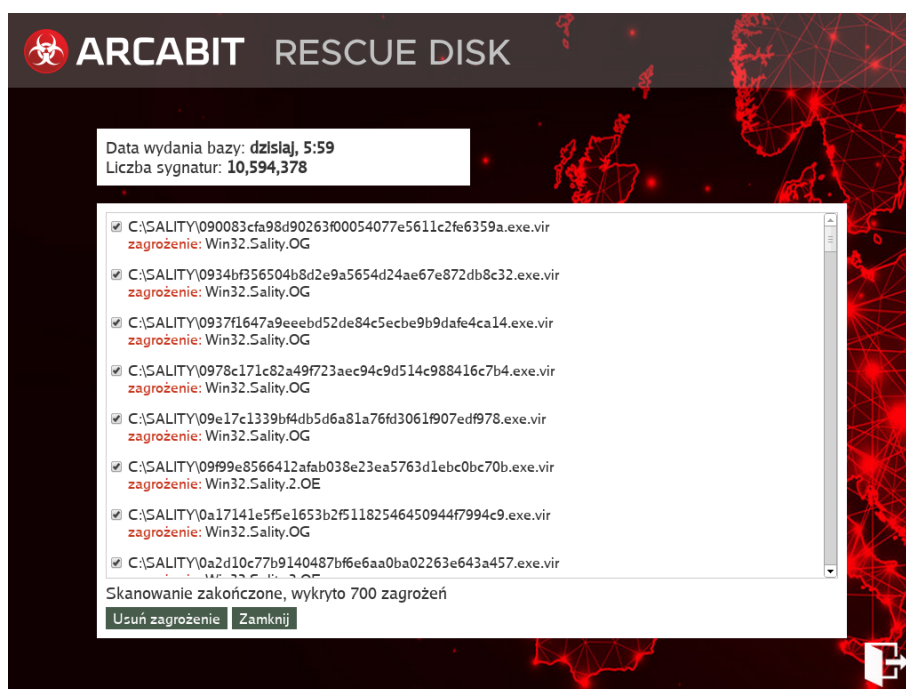
Po zaznaczeniu dysków, które chcemy przeskanować i wybraniu „Skanuj” rozpocznie się proces skanowania; w przypadku znalezienia jakiegoś zagrożenia pojawi się ono na liście, która w miarę ew. znajdowania innych zagrożeń może się wypełniać:



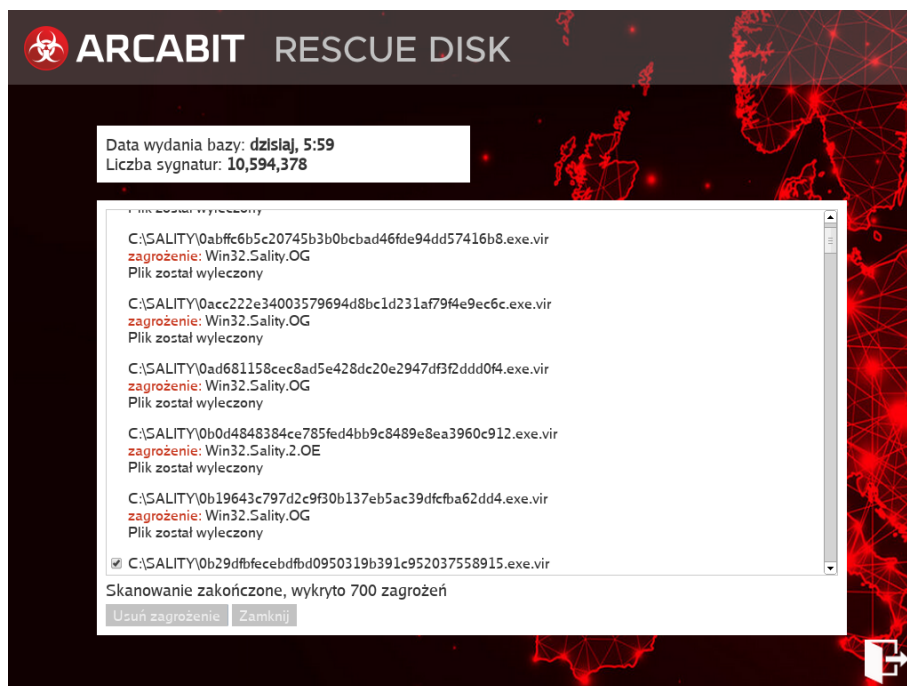
Po zakończeniu skanowania zaznaczonych uprzednio dysków, w przypadku gdy nie zostanie znalezione żadne zagrożenie, pojawi się komunikat:



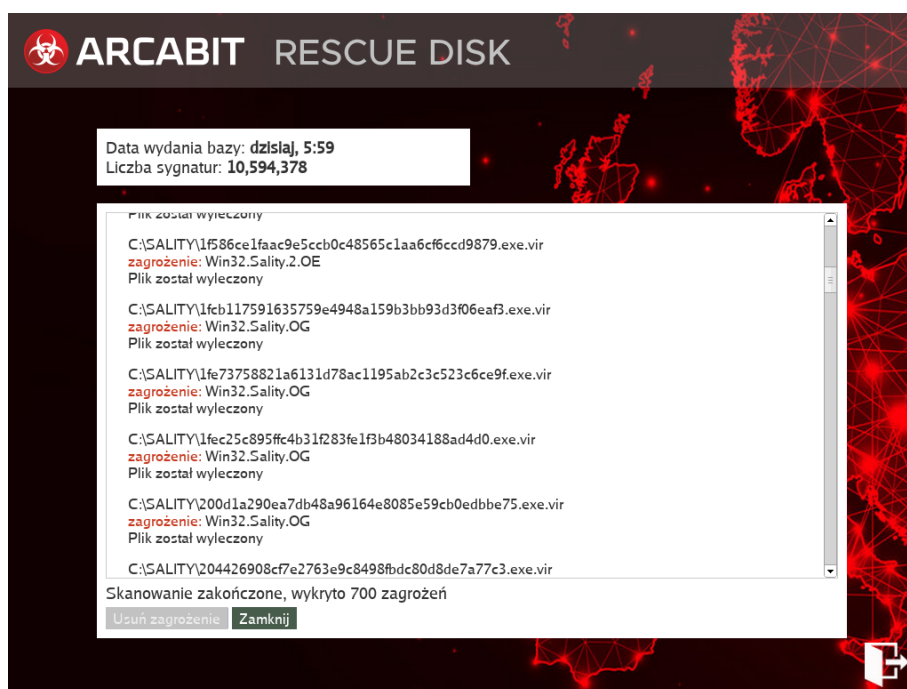
natomiast w przypadku znalezienia zagrożeń pojawi się możliwość ich usunięcia przez wybranie „Usun zagrożenia”:



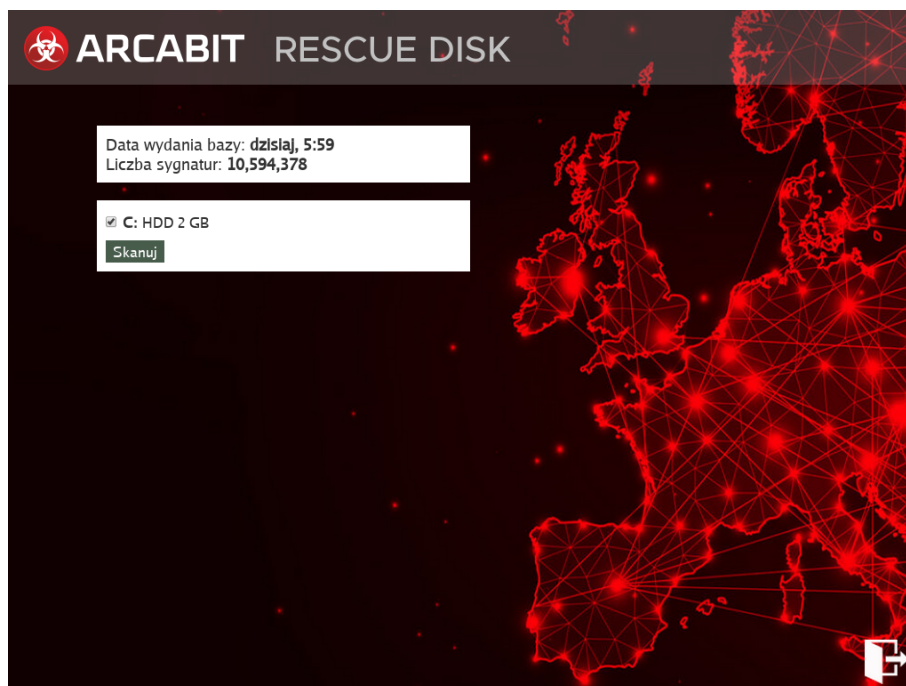
Po wybraniu „Usun zagrożenia” rozpocznie się proces ich usuwania, przy czym jeśli to będą wirusy infekujące pliki, takie pliki będą leczone, natomiast w przeciwnym wypadku (konie trojańskie, robaki itp.) wykryte jako zagrożenia pliki będą nieodwracalnie kasowane:



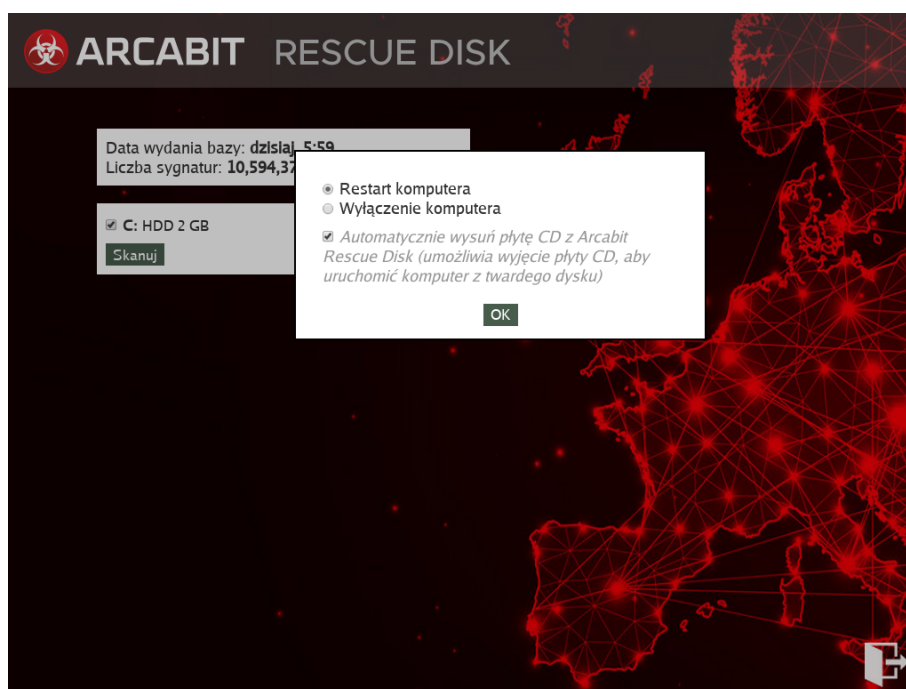
Po zakończeniu usuwania zagrożeń pojawi się okno z raportem, w którym można zobaczyć, które z zainfekowanych plików zostały wyleczone, a które skasowane:



Wybranie „Zamknij” powoduje powrót do startowego okna „Rescue Disk”:



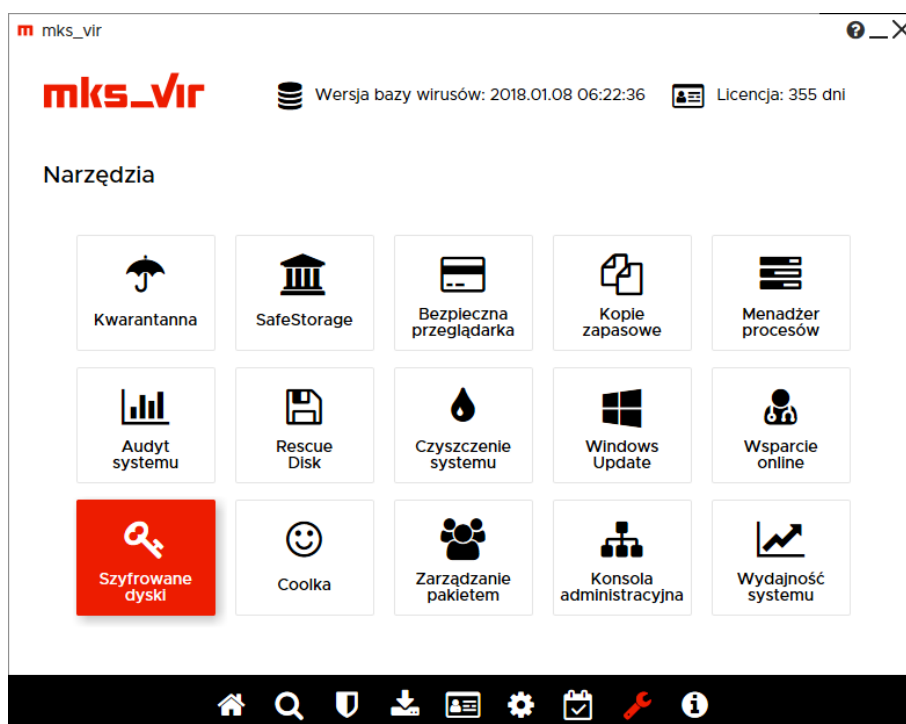
Wybranie zamknięcia „Rescue Disk” (ikona w prawym, dolnym narożniku) powoduje pojawienie się komunikatu:



który pozwala na wybranie, czy komputer ma zostać wyłączony, czy uruchomiony ponownie (restart) - po zaznaczeniu właściwej i wybraniu „OK” komputer zostanie albo wyłączony, albo uruchomiony ponownie. Dodatkowa opcja pozwalająca na automatyczne wysunięcie płyty z napędu ma znaczenie tylko w przypadku uruchomienia nośnika ratunkowego „Rescue Disk” z płyty CD/DVD.

Zarządzanie szyfrowanymi dyskami

Dostęp do obsługi *szyfrowanych dysków* w programie **mks_vir** jest poprzez sekcję „Narzędzia → Szyfrowane dyski” w głównym oknie:

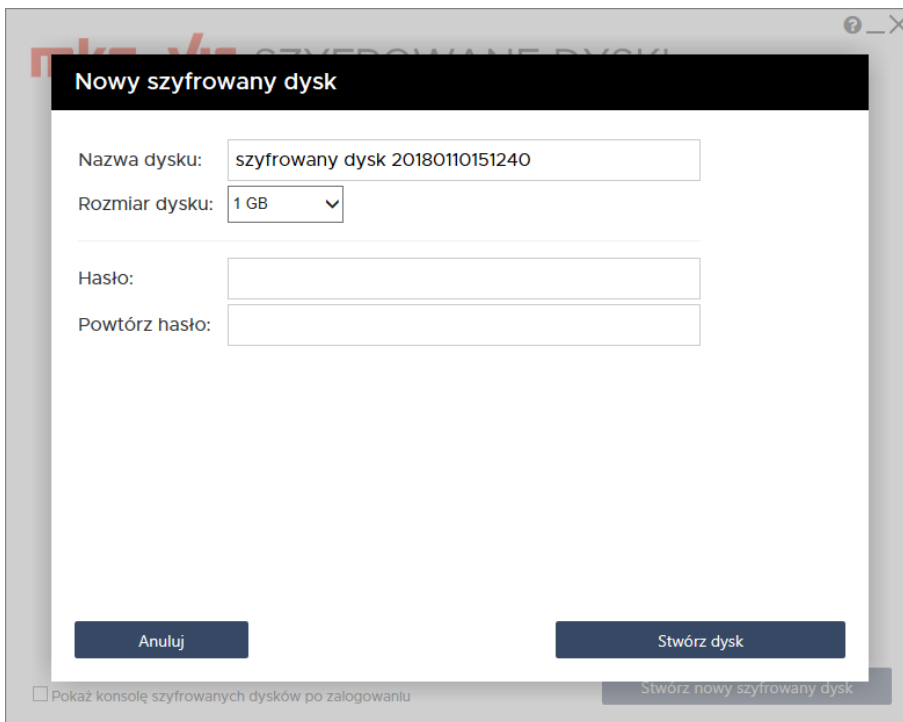


Po jego wybraniu pojawi się okno konsoli do zarządzania *szyfrowanymi dyskami*:

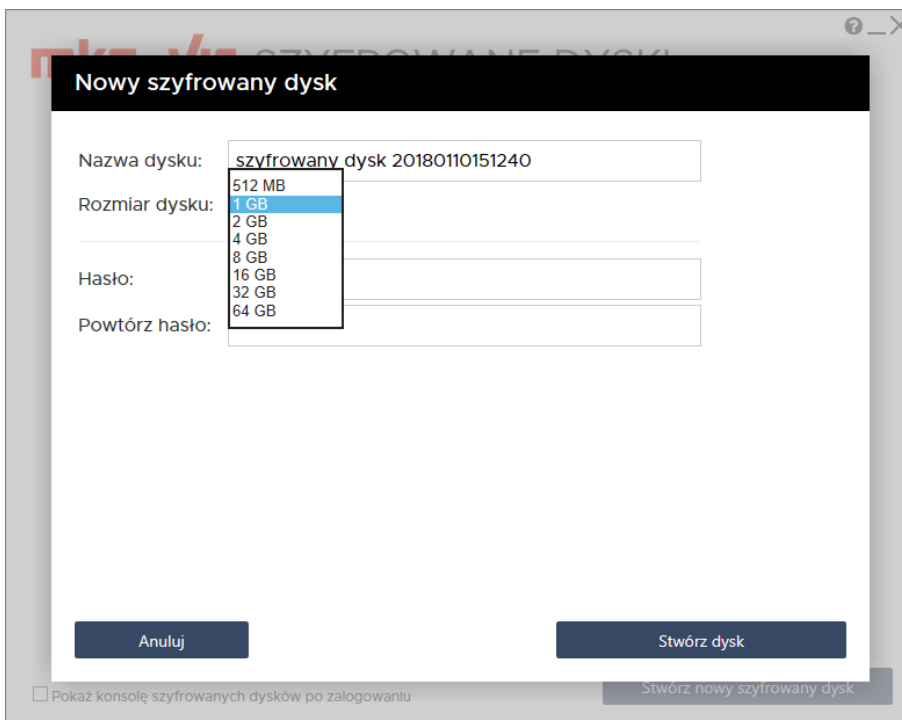


Opcja „Pokaż konsolę szyfrowanych dysków po zalogowaniu” pozwala na automatyczne wyświetlenie okna konsoli zaraz po zalogowaniu się użytkownika, dzięki czemu można od razu podłączyć własne *szyfrowane dyski*

Wybranie „Stwórz nowy szyfrowany dysk” umożliwi utworzenie *szyfrowanego dysku* i dostosowanie jego parametrów:



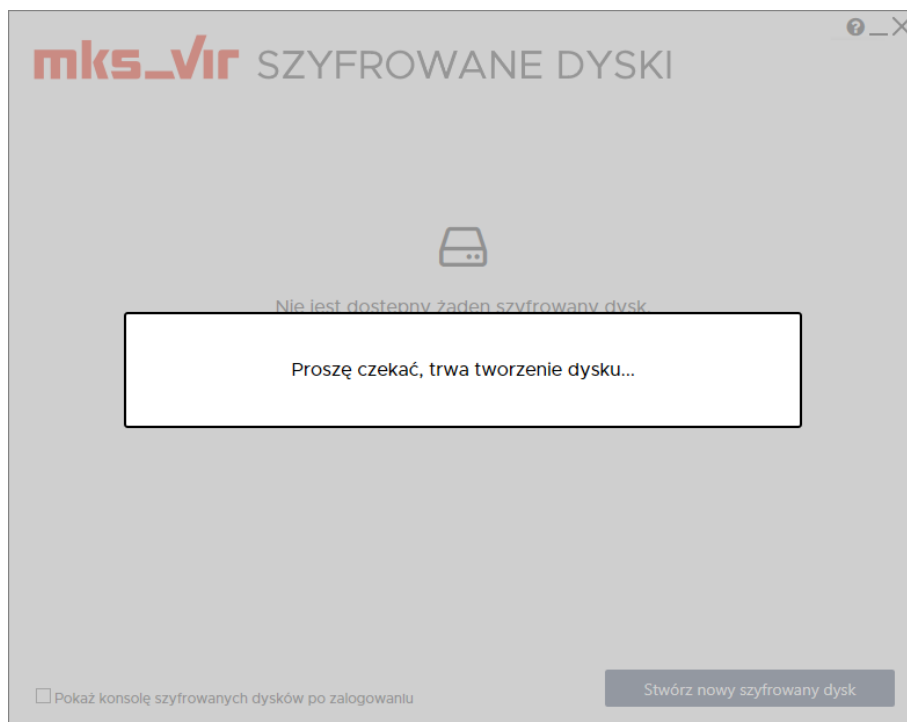
- **Nazwa dysku** – pozwala na wybranie własnej nazwy pliku z zawartością *szyfrowanego dysku* (będzie także domyślnie ustawioną etykietą takiego dysku)
- **Rozmiar dysku** – pozwala na wybranie pojemności *szyfrowanego dysku*; pojemność wybiera się spośród kilku możliwości (512 MB, 1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB i 64 GB):



- **Hasło** – zabezpiecza przed nieautoryzowanym podłączeniem *szyfrowanego dysku*; jego podanie jest konieczne przy każdym podłączaniu dysku






UWAGA! Hasło nie jest nigdzie zapamiętywane w programie, jego utrata/zapomnienie uniemożliwia dostęp do danych zapisanych na takim *szyfrowanym dysku*!

Po dostosowaniu parametrów, wpisaniu i powtórzeniu hasła zabezpieczającego wybieramy „Stwórz dysk” aby utworzyć *szyfrowany dysk*; procedura tworzenia dysku może trochę trwać, czas jest zależny od wielkości tworzonego dysku, szybkości procesora i dysku twardego, na którym jest tworzony plik *szyfrowanego dysku*:

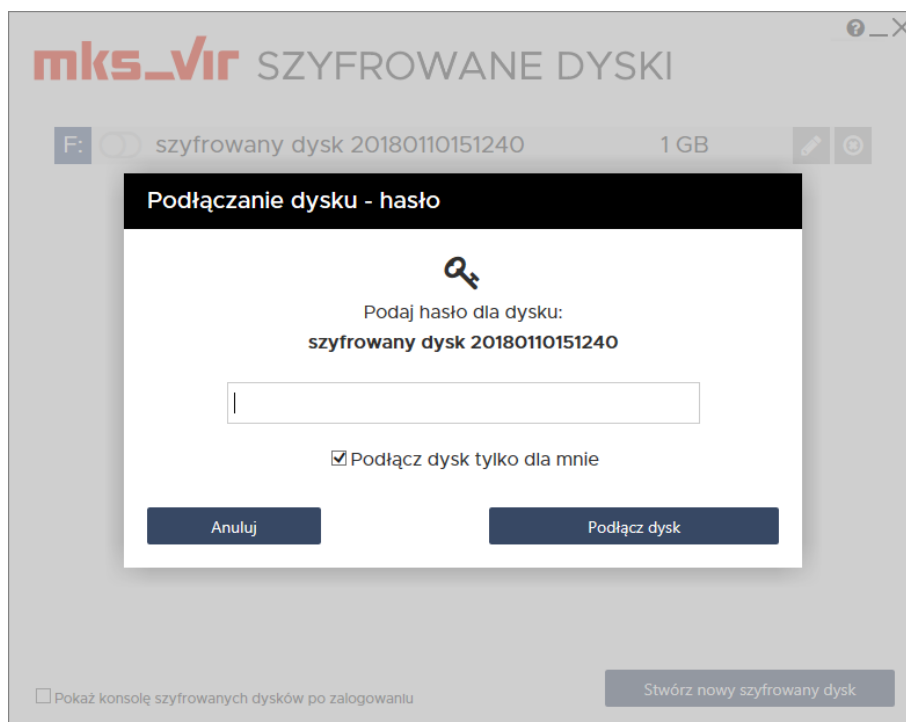


Po utworzeniu dysku pojawia się on na liście dostępnych *szyfrowanych dysków*:




- Kliknięcie w literę dysku umożliwia zmianę przyporządkowania litery *szyfrowanego dysku* pod jaką będzie on widoczny w systemie po podłączeniu
-  – umożliwia podłączenie lub odłączenie *szyfrowanego dysku*, zależnie od jego aktualnego stanu ( – niepodłączony czy  – podłączony)
-  – umożliwia zmianę nazwy *szyfrowanego dysku*
-  – umożliwia skasowanie *szyfrowanego dysku* (skasowanie dysku powoduje fizyczne usunięcie pliku dysku wraz z zawartymi na nim danymi, co uniemożliwia ich ew. odzyskanie)

Wybranie ikony podłączenia *szyfrowanego dysku* powoduje wyświetlenie okna do wpisania hasła podanego w czasie tworzenia dysku:



Po jego wpisaniu i wybraniu „Podłącz dysk” *szyfrowany dysk* zostaje podłączony i jego zawartość staje się widoczna dla systemu jako dysk o literze przypisanej do danego *szyfrowanego dysku*

Wybranie opcji „Podłącz dysk tylko dla mnie” powoduje, że zawartość *szyfrowanego dysku* jest dostępna tylko dla użytkownika, który utworzył i podłączył dany dysk; jeśli opcja nie jest wybrana, zawartość *szyfrowanego dysku* jest dostępna dla wszystkich użytkowników zalogowanych w systemie

W konsoli do zarządzania *szyfrowanymi dyskami* stan, gdy dysk jest podłączony, jest sygnalizowany ikonką :

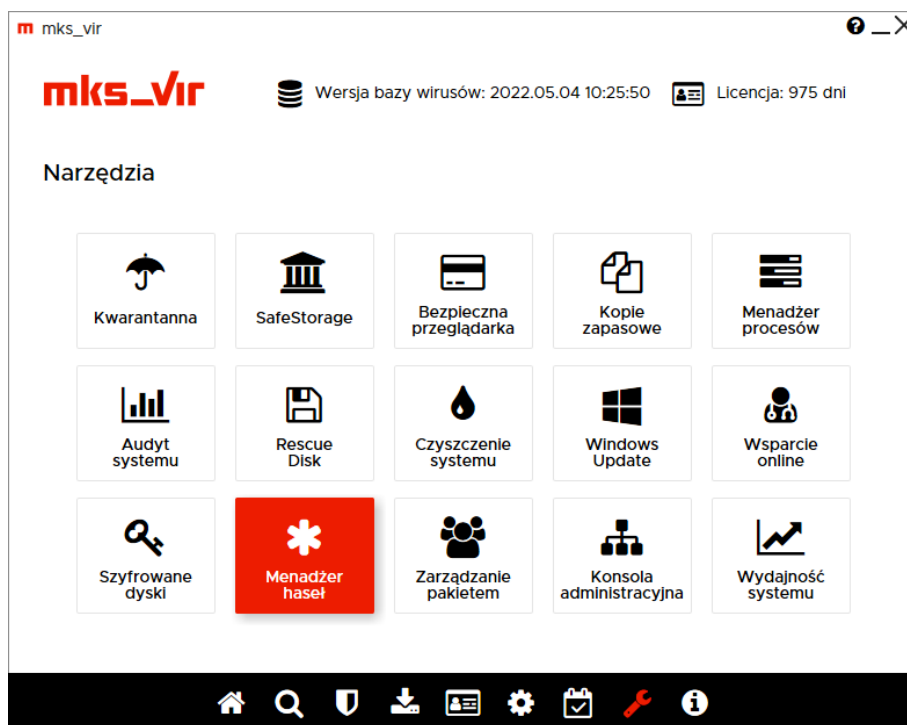


Kliknięcie w nią odłącza *szyfrowany dysk*, co równocześnie zabezpiecza zawarte na nim dane przed ew. niepowołanym dostępem

Korzystanie z menadżera haseł

Menadżer haseł w programie **mks_vir** umożliwia bezpieczne przechowywanie, korzystanie i generowanie silnych haseł do różnych usług (bankowych, portali społecznościowych itp.)

Dostęp do *menadżera haseł* w programie **mks_vir** jest poprzez sekcję „Narzędzia → Menadżer haseł” w głównym oknie:

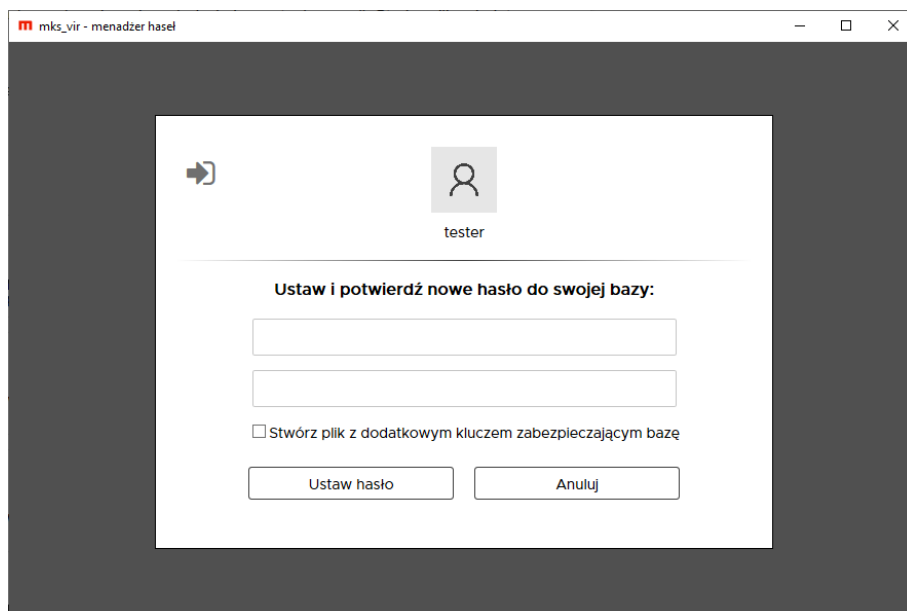


Przy pierwszym uruchomieniu *menadżera haseł* pojawi się okno do ustawienia własnego hasła chroniącego dostęp do zgromadzonych w *menadżerze haseł* danych. Hasło powinno być na tyle skomplikowane, by nie można go było łatwo odgadnąć, a jednocześnie łatwe do zapamiętania dla użytkownika, gdyż zapomnienie tego hasła powoduje nieodwracalną utratę dostępu do zgromadzonych w *menadżerze haseł* danych

Dodatkowym zabezpieczeniem danych może być skorzystanie z opcji „Stwórz plik z dodatkowym kluczem zabezpieczającym bazę” – wybranie tej opcji spowoduje zapisanie w wybranej przez użytkownika lokalizacji pliku z kluczem

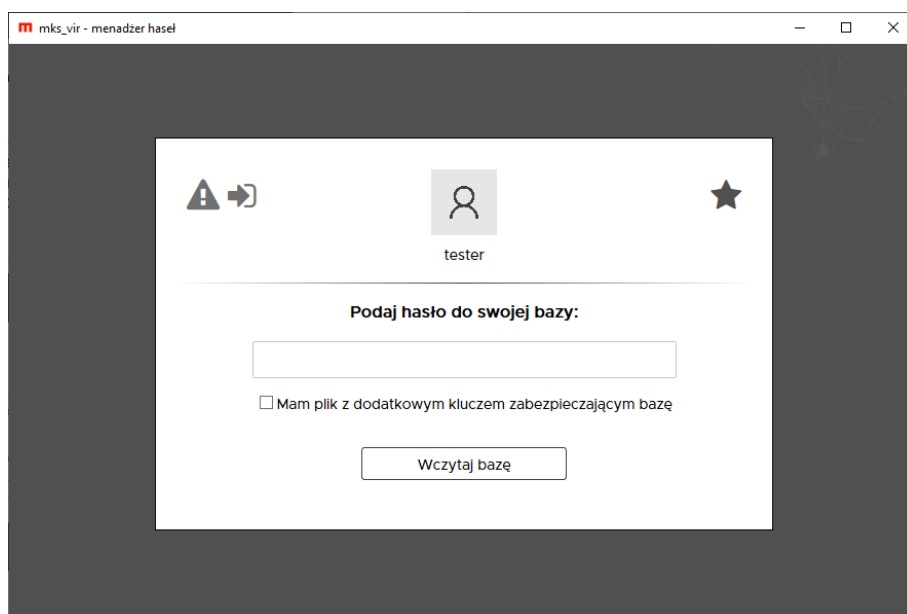
UWAGA! Utrata pliku klucza, w przypadku gdy z niego korzystamy, spowoduje jednocześnie utratę dostępu do zgromadzonych w menadżerze haseł danych

Wybranie „Ustaw hasło” powoduje stworzenie pustej bazy, do której dostęp będzie możliwy przez podanie własnego hasła, a jeśli zaznaczymy opcję „Stwórz plik z dodatkowym kluczem zabezpieczającym bazę”, także zapisanie pliku z dodatkowym kluczem zabezpieczającym:



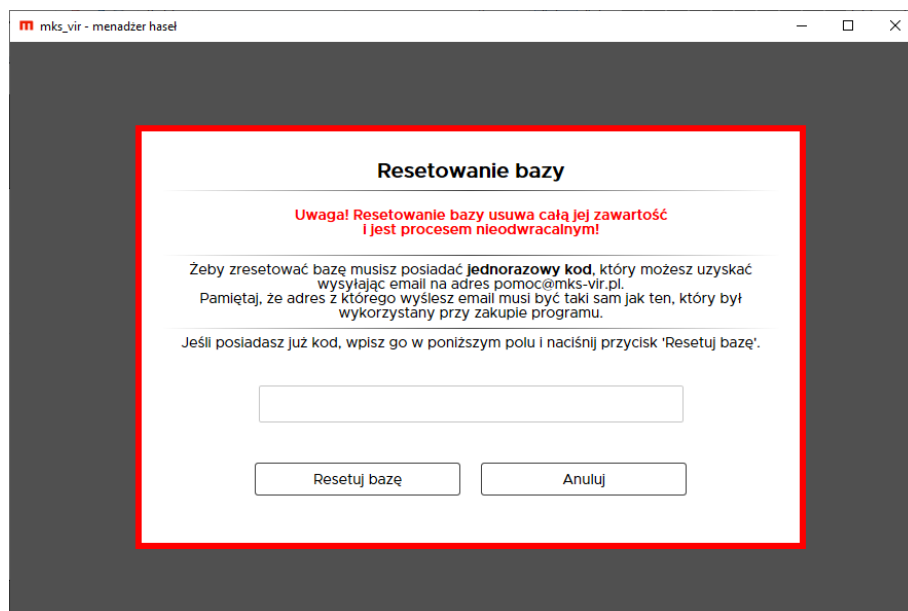
- ➡ – **importuj swoją bazę** – umożliwia wczytanie swojej bazy danych z uprzednio zapamiętanej kopii zapasowej pliku bazy

W przypadku, gdy baza *menadżera hasel* została już wcześniej utworzona, zostanie otwarte okno umożliwiające podanie hasła zabezpieczającego dostęp do danych zgromadzonych w *menadżerze hasel* – jeśli przy tworzeniu hasła zabezpieczającego utworzyliśmy plik klucza zabezpieczającego, należy zaznaczyć opcję „Mam plik z dodatkowym kluczem zabezpieczającym bazę”. Po wpisaniu hasła należy wybrać „Wczytaj bazę”:

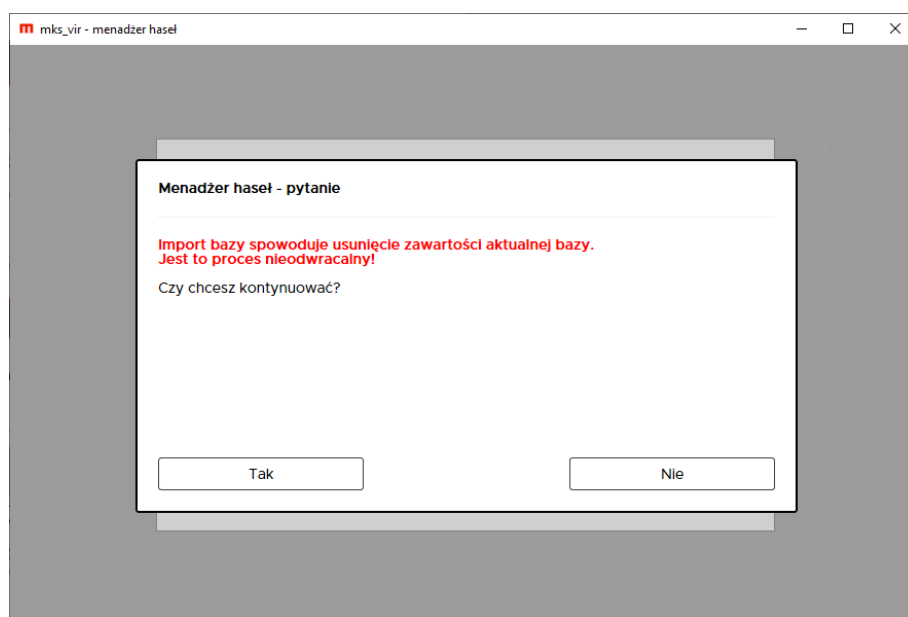


Dodatkowe ikony umożliwiają:

- ⚠ – **resetuj swoją bazę** – umożliwia usunięcie bazy danych w przypadku utraty możliwości dostępu do tych danych, np. w przypadku zapomnienia hasła lub utraty pliku klucza zabezpieczającego (jeśli z niego korzystamy):

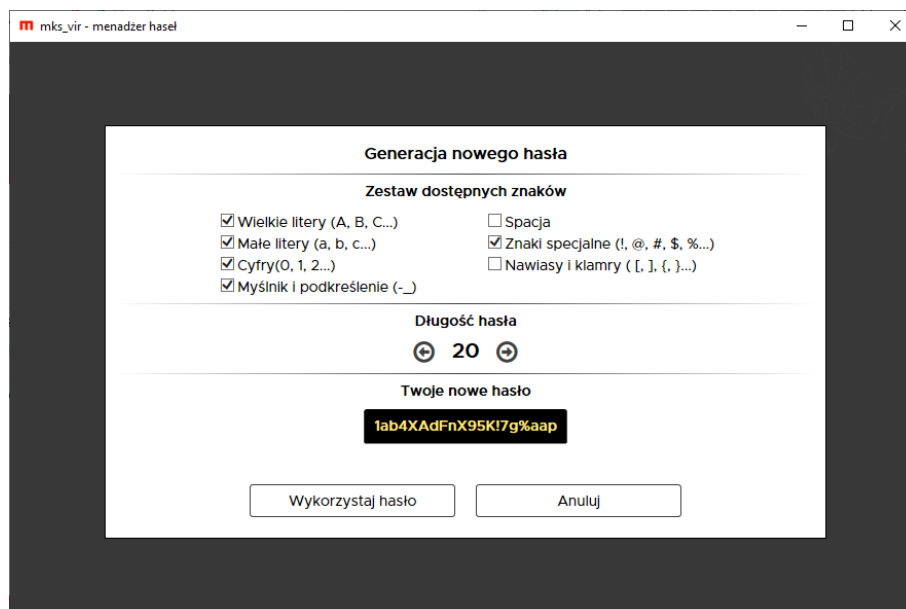


- ➔ – **importuj swoją bazę** – umożliwia wczytanie swojej bazy danych z uprzednio zapamiętanej kopii zapasowej pliku bazy

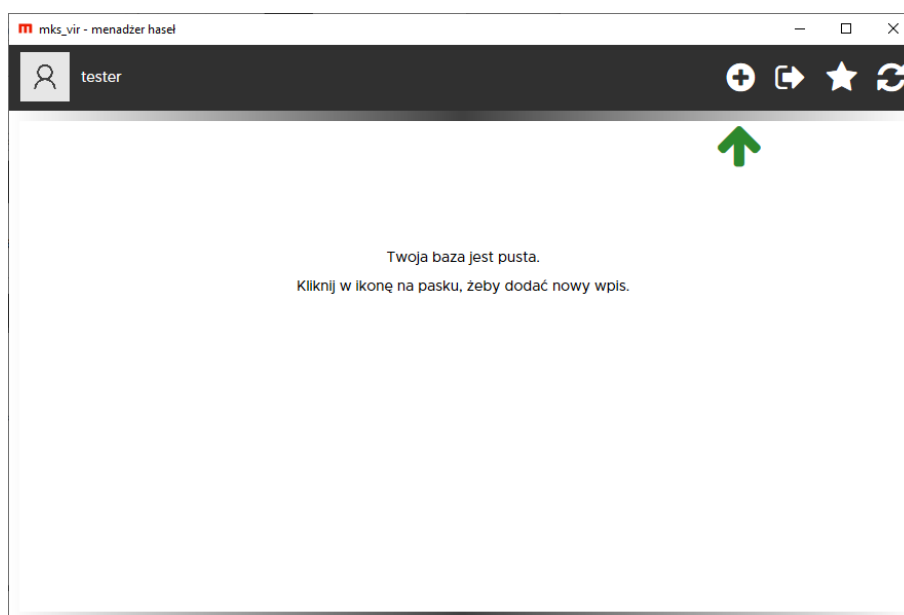


- ★ – **wygeneruj hasło bez logowania** – umożliwia wygenerowanie hasła bez konieczności otwierania bazy danych *menadżera haseł*
 - **Zestaw dostępnych znaków** – pozwala na określenie z jakich typów znaków (z kilku grup) ma składać się generowane hasło
 - **Długość hasła** – pozwala na określenie jaką długość w znakach ma mieć generowane hasło
 - **Twoje nowe hasło** – wyświetla podgląd aktualnie wygenerowanego hasła

wybranie „Wykorzystaj hasło” powoduje skopiowanie hasła do schowka systemowego:

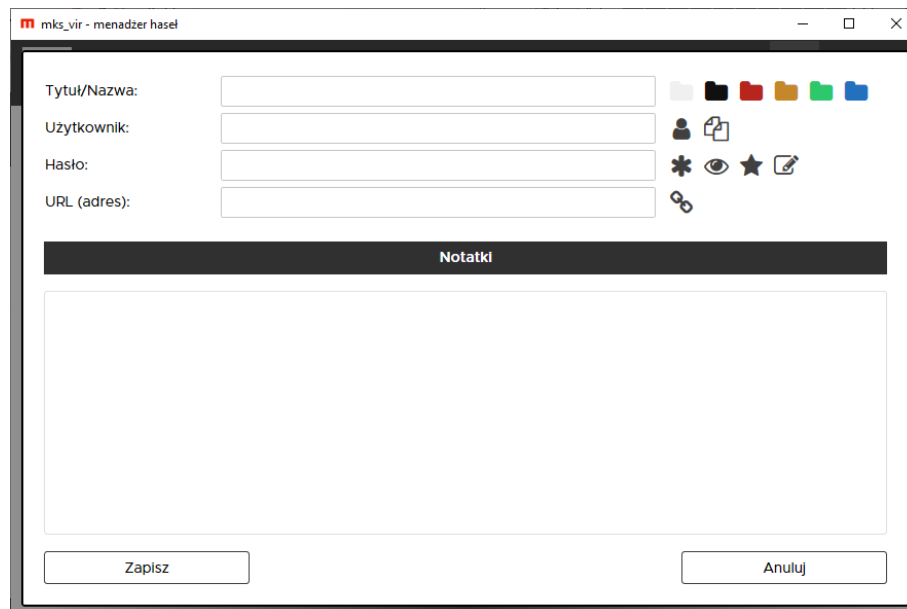


Pierwsze otwarcie bazy danych *menadżera haseł* wyświetli okno bez żadnych wpisów:



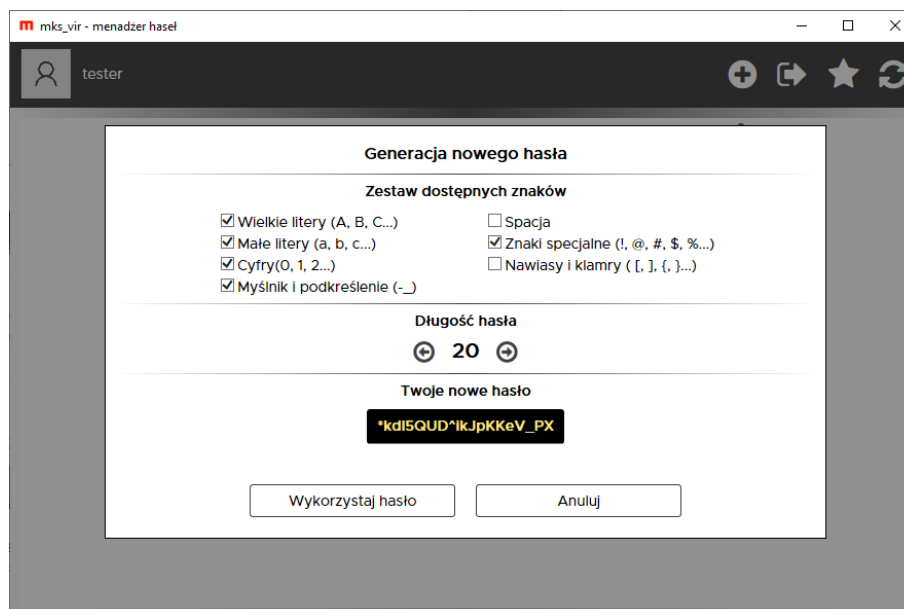
Poszczególne ikony widoczne po prawej stronie u góry okna umożliwiają:

- **Nowy wpis** – dodanie nowego wpisu do bazy *menadżera haseł*; wybranie „Zapisz” powoduje zapisanie wpisu w bazie danych *menadżera haseł*:

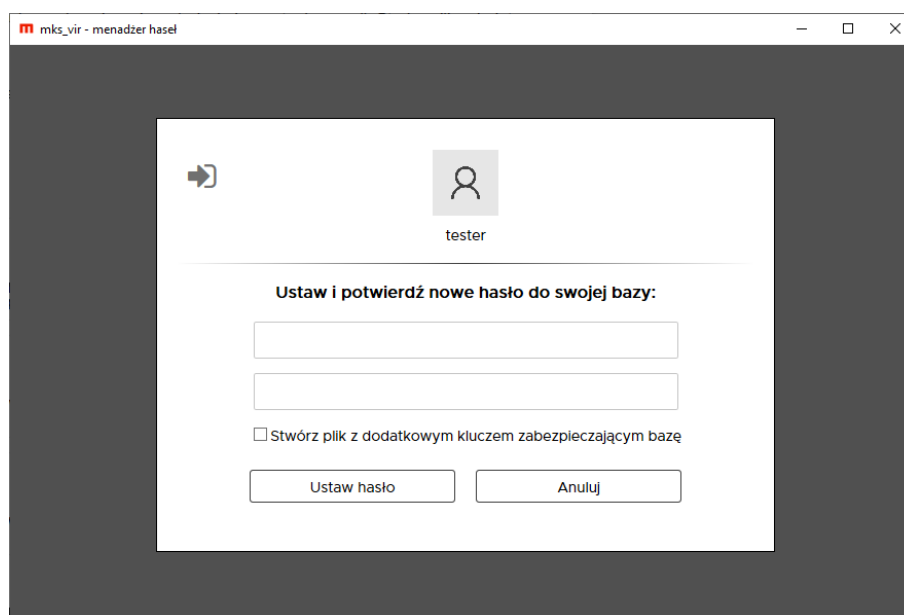


- **Tytuł/Nazwa** – pozwala na określenie pod jaką nazwą wpis z danymi logowania do konkretnej usługi będzie widoczny na liście pozycji bazy danych *menadżera haseł*; ikony po prawej stronie pozwalają na wybór koloru dla danego wpisu
 - **Użytkownik** – pole do wpisania użytkownika/nazwy konta za pomocą którego logujemy się do konkretnej usługi; ikony po prawej stronie pozwalają na skopiowanie zawartości pola lub wysłanie sekwencji logującej dla zdefiniowanej usługi
 - **Hasło** – pole do wpisania hasła logującego do konkretnej usługi; ikony po prawej stronie pozwalają na skopiowanie hasła, podejrzenie/ukrycie hasła, wygenerowanie silnego hasła dla zdefiniowanej usługi lub odblokowanie możliwości ręcznej edycji hasła
 - **URL (adres)** – pole do wpisania adresu www dla konkretnej usługi; ikona po prawej stronie pozwala na otwarcie strony zdefiniowanej usługi w domyślnej przeglądarce internetowej
 - **Notatki** – pole do wpisania notatek o dowolnej treści
- **Eksportuj bazę danych** – umożliwia wykonanie kopii zapasowej pliku bazy danych
 - **Generuj hasło** – wygenerowanie hasła bez konieczności tworzenia nowego wpisu w bazie *menadżera haseł*
 - **Zestaw dostępnych znaków** – pozwala na określenie z jakich typów znaków (z kilku grup) ma składać się generowane hasło
 - **Długość hasła** – pozwala na określenie jaką długość w znakach ma mieć generowane hasło
 - **Twoje nowe hasło** – wyświetla podgląd aktualnie wygenerowanego hasła

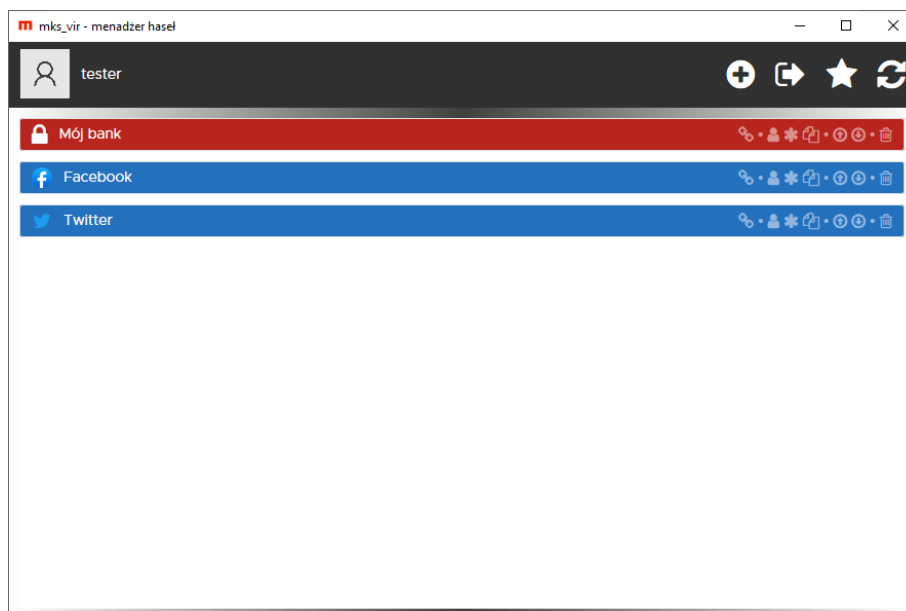
wybranie „Wykorzystaj hasło” powoduje skopiowanie hasła do schowka systemowego:



- **Zmień hasło do swojej bazy** – zmiana hasła (oraz klucza zabezpieczającego, jeśli z niego korzystamy) do bazy danych *menadżera haseł*:



Otwarcie bazy danych *menadżera haseł* ze zdefiniowanymi wcześniej wpisami wyświetli okno:

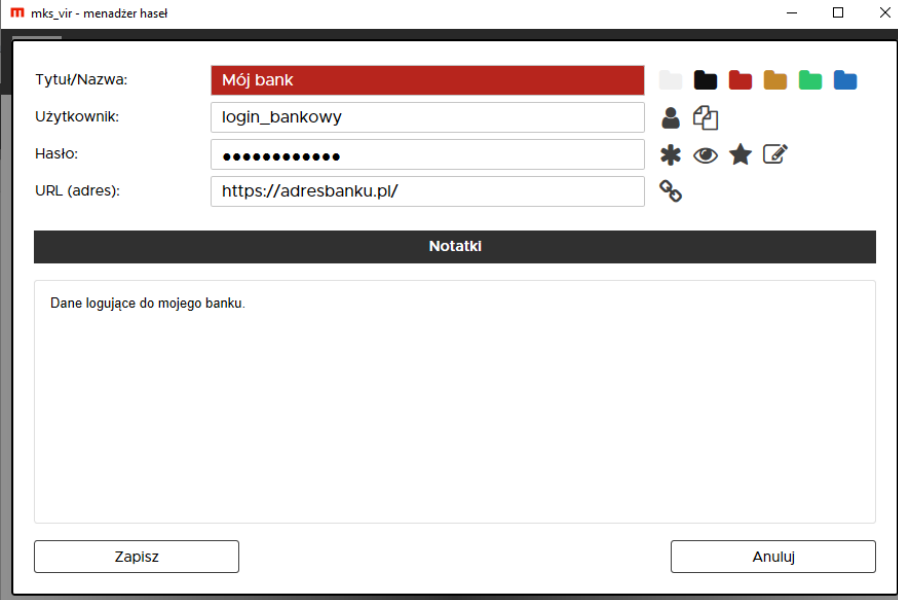


Poszczególne ikony widoczne po prawej stronie paska danego wpisu umożliwiają:

- **Otwórz stronę** – otwiera stronę www zdefiniowanej usługi w domyślnej przeglądarce internetowej
- **Kopiuje nazwę użytkownika** – kopiuje nazwę użytkownika dla zdefiniowanej usługi do schowka systemowego
- **Kopiuje hasło** – kopiuje hasło dla zdefiniowanej usługi do schowka systemowego
- **Kopiuje sekwencję** – kopiuje sekwencję logującą dla zdefiniowanej usługi do schowka systemowego
- **Do góry** – przesuwa zdefiniowany wpis w górę listy
- **W dół** – przesuwa zdefiniowany wpis w dół listy
- **Usuń ten wpis** – usuwa wybrany wpis z bazy danych *menadżera haseł*

UWAGA! Usunięcie wpisu z bazy jest nieodwracalne, aby go przywrócić należy zdefiniować go na nowo

Kliknięcie w zdefiniowany wpis wyświetla okno pozwalające na modyfikację poszczególnych elementów wpisu dotyczącego konkretnej usługi:



The screenshot displays a window titled "mks_vir - menadżer haseł". The main area contains a form for a saved login entry:

- Tytuł/Nazwa: **Mój bank** (highlighted in red)
- Użytkownik: login_bankowy
- Hasło: ••••••••
- URL (adres): https://adresbanku.pl/

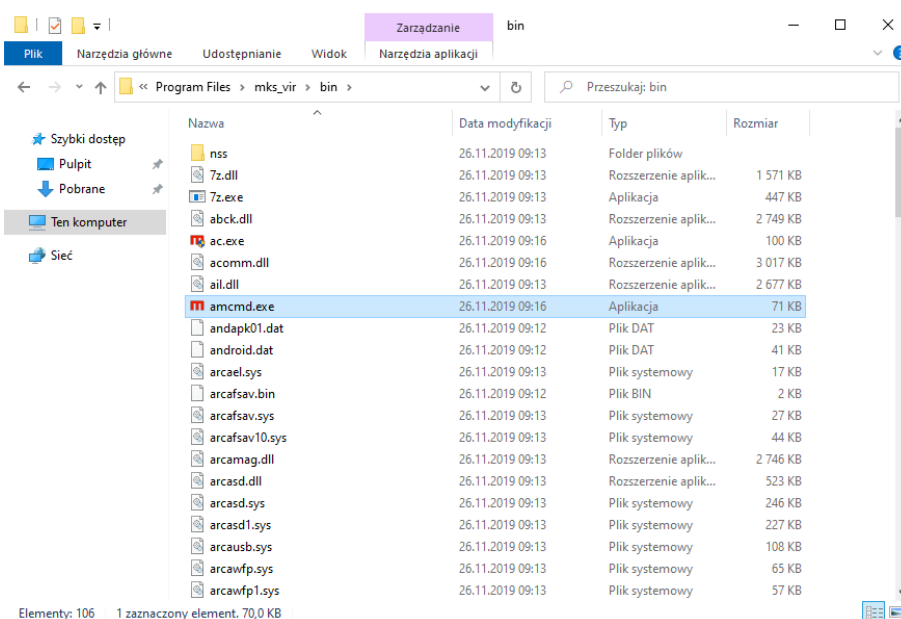
To the right of the form are several icons: a folder icon, a person icon, a document icon, a star icon, a pencil icon, and a scissors icon.

Below the form is a section titled "Notatki" (Notes) with a text area containing the text: "Dane logujące do mojego banku."

At the bottom of the window are two buttons: "Zapisz" (Save) and "Anuluj" (Cancel).

Korzystanie ze skanera command line

W programie **mks_vir** jest możliwość skorzystania ze skanera *command line*, służy do tego program „amcmd” znajdujący się w folderze (domyślnie) c:\program files\mks_vir\bin:



Skaner *command line* programu **mks_vir** pozwala na skanowanie zawartości folderów lub pojedynczych plików

Aby przeskanować zawartość folderu za pomocą skanera *command line* programu **mks_vir**, należy w oknie linii poleceń systemu Windows „cmd” wpisać komendę:

```
"c:\program files\mks_vir\bin\amcmd.exe" folder
```

(w przykładzie jest to folder c:\users\tester\desktop\test), po czym wcisnąć klawisz „enter”, co rozpocznie skanowanie zawartości folderu:

```
C:\Windows\system32\cmd.exe - "c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test
C:\Users\tester>"c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test
c:\Users\tester\Desktop\test\00000001.vir      INFECTED      Win32.Worm.Allapple.Gen
c:\Users\tester\Desktop\test\00000002.vir      INFECTED      Trojan.Generic
c:\Users\tester\Desktop\test\00000003.vir      INFECTED      Trojan.Generic.D27986F6
c:\Users\tester\Desktop\test\00000004.vir      INFECTED      Trojan.A
c:\Users\tester\Desktop\test\00000005.vir      INFECTED      Trojan.A
c:\Users\tester\Desktop\test\00000006.vir      INFECTED      Win32.Worm.Allapple.Gen
c:\Users\tester\Desktop\test\00000007.vir      INFECTED      Win32.Worm.Allapple.Gen
c:\Users\tester\Desktop\test\00000008.vir      INFECTED      Trojan.Generic.D27986F6
```

- **INFECTED** – oznacza, że przeskanowany plik jest zainfekowany
- **CLEAN** – oznacza, że przeskanowany plik jest czysty

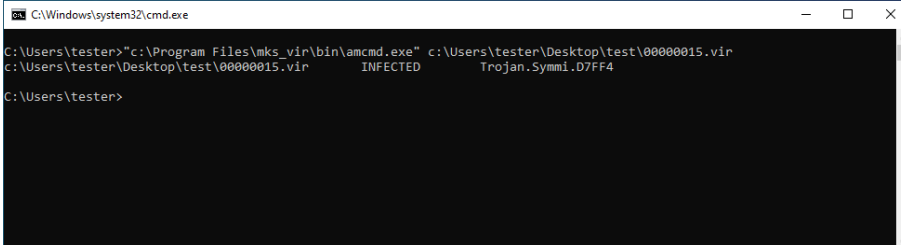
Wyniki skanowania zamiast na ekran mogą być zapisywane do pliku, wystarczy w tym celu przekierować strumień wynikowy z ekranu na plik (przez dopisanie na końcu > plik.txt):

```
"c:\program files\mks_vir\bin\amcmd.exe" folder > plik.txt
```

Aby przeskanować pojedynczy plik za pomocą skanera *command line* programu **mks_vir**, należy w oknie linii poleceń systemu Windows „cmd” wpisać komendę:

```
"c:\program files\mks_vir\bin\amcmd.exe" ścieżka_do_pliku
```

(w przykładzie jest to plik `c:\users\tester\desktop\test\00000015.vir`), po czym wcisnąć klawisz „*enter*”, co rozpocznie skanowanie pliku:



```
C:\Windows\system32\cmd.exe
C:\Users\tester>"c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test\00000015.vir
c:\Users\tester\Desktop\test\00000015.vir      INFECTED      Trojan.Symmi.D7FF4
C:\Users\tester>
```

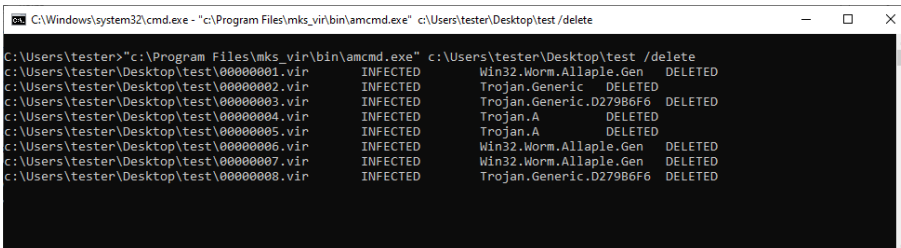
Wynik skanowania zamiast na ekran może być zapisany do pliku przez przekierowanie strumienia wynikowego z ekranu na plik (przez dopisanie na końcu `> plik.txt`)

Skanowanie zawartości folderów lub plików tak jak wyżej nie powoduje wykonania żadnej akcji po znalezieniu zainfekowanych plików. Aby usunąć zainfekowane pliki należy do linii poleceń dodać dodatkowy parametr `/delete`

Aby przeskanować zawartość folderu za pomocą skanera *command line* programu **mks_vir** wykonując automatyczne usuwanie znalezionych zainfekowanych plików, należy w oknie linii poleceń systemu Windows „cmd” wpisać komendę:

```
"c:\program files\mks_vir\bin\amcmd.exe" folder /delete
```

(w przykładzie jest to folder `c:\users\tester\desktop\test`), po czym wcisnąć klawisz „*enter*”, co rozpocznie skanowanie zawartości folderu:



```
C:\Windows\system32\cmd.exe - "c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test /delete
C:\Users\tester>"c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test /delete
c:\Users\tester\Desktop\test\00000001.vir      INFECTED      Win32.Worm.Allapple.Gen      DELETED
c:\Users\tester\Desktop\test\00000002.vir      INFECTED      Trojan.Generic               DELETED
c:\Users\tester\Desktop\test\00000003.vir      INFECTED      Trojan.Generic.D279B6F6      DELETED
c:\Users\tester\Desktop\test\00000004.vir      INFECTED      Trojan.A                      DELETED
c:\Users\tester\Desktop\test\00000005.vir      INFECTED      Trojan.A                      DELETED
c:\Users\tester\Desktop\test\00000006.vir      INFECTED      Win32.Worm.Allapple.Gen      DELETED
c:\Users\tester\Desktop\test\00000007.vir      INFECTED      Win32.Worm.Allapple.Gen      DELETED
c:\Users\tester\Desktop\test\00000008.vir      INFECTED      Trojan.Generic.D279B6F6      DELETED
```

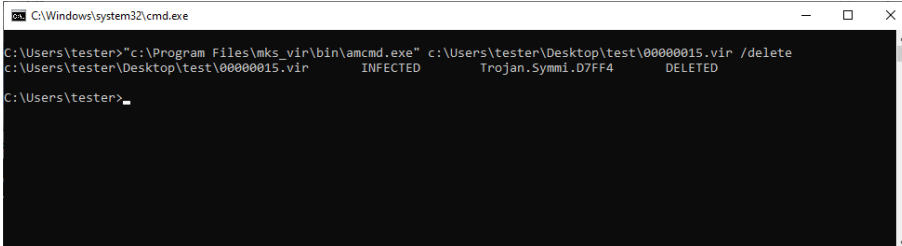
- **DELETED** – oznacza, że przeskanowany plik został usunięty

Wyniki skanowania zamiast na ekran mogą być zapisane do pliku przez przekierowanie strumienia wynikowego z ekranu na plik (przez dopisanie na końcu `> plik.txt`)

Aby przeskanować pojedynczy plik za pomocą skanera *command line* programu **mks_vir** wykonując automatyczne usunięcie pliku jeśli okazał się zainfekowany, należy w oknie linii poleceń systemu Windows „cmd” wpisać komendę:

```
"c:\program files\mks_vir\bin\amcmd.exe" ścieżka_do_pliku /delete
```

(w przykładzie jest to plik `c:\users\tester\desktop\test\00000015.vir`), po czym wcisnąć klawisz „*enter*”, co rozpocznie skanowanie pliku:



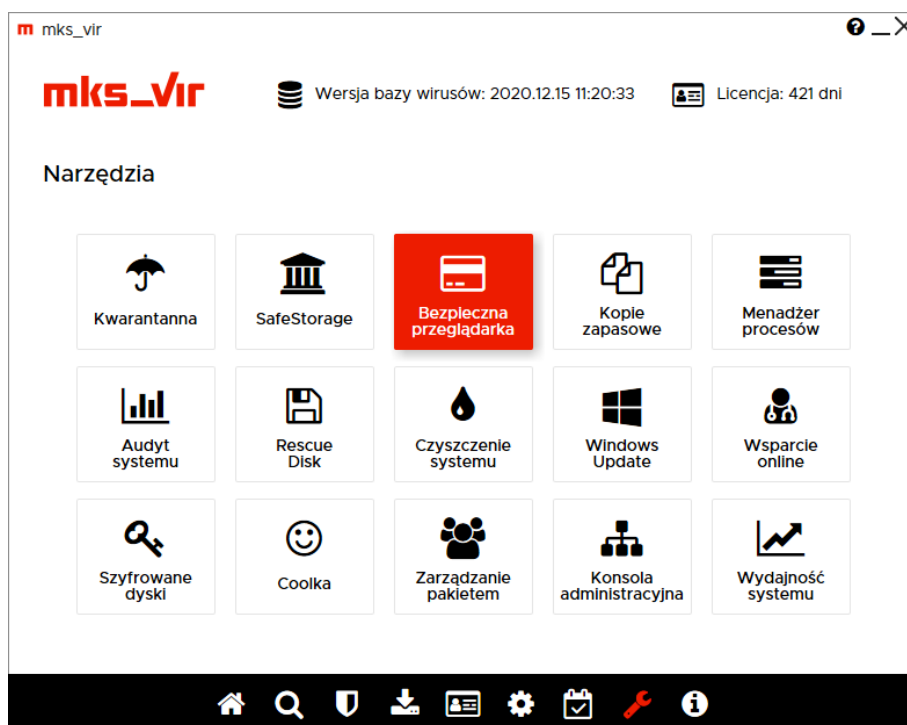
```
C:\Windows\system32\cmd.exe
C:\Users\tester>"c:\Program Files\mks_vir\bin\amcmd.exe" c:\Users\tester\Desktop\test\00000015.vir /delete
c:\Users\tester\Desktop\test\00000015.vir      INFECTED      Trojan.Symmi.D7FF4      DELETED
C:\Users\tester>
```

Wynik skanowania zamiast na ekran może być zapisany do pliku przez przekierowanie strumienia wynikowego z ekranu na plik (przez dopisanie na końcu `> plik.txt`)

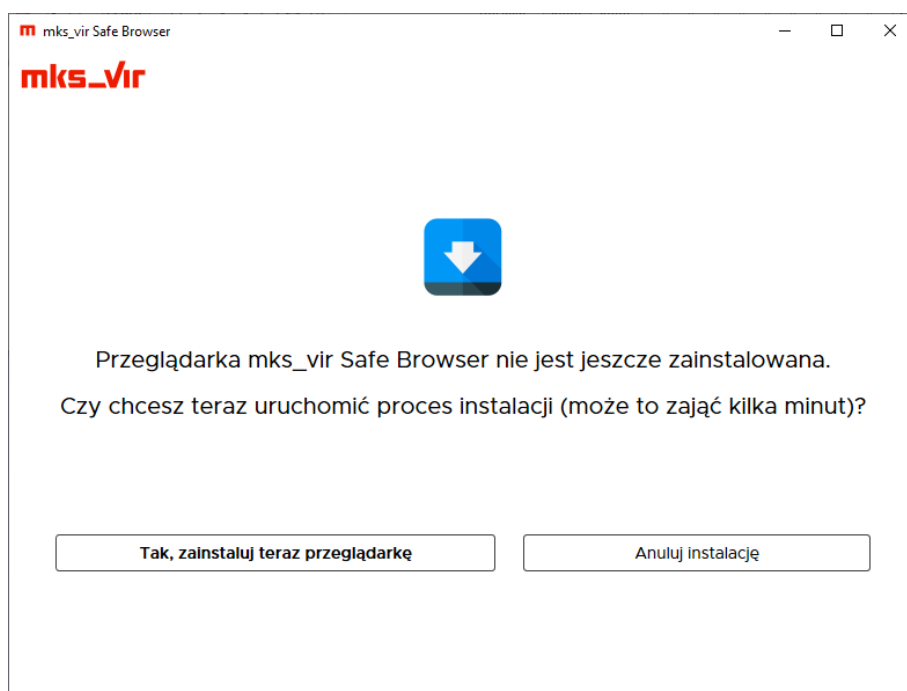
Korzystanie z bezpiecznej przeglądarki

Bezpieczna przeglądarka w programie **mks_vir** to przeglądarka zapewniająca wysoki poziom bezpieczeństwa w trakcie korzystania z zasobów Internetu, a zwłaszcza w trakcie operacji bankowych, płatniczych oraz wymagających podawania wrażliwych danych.

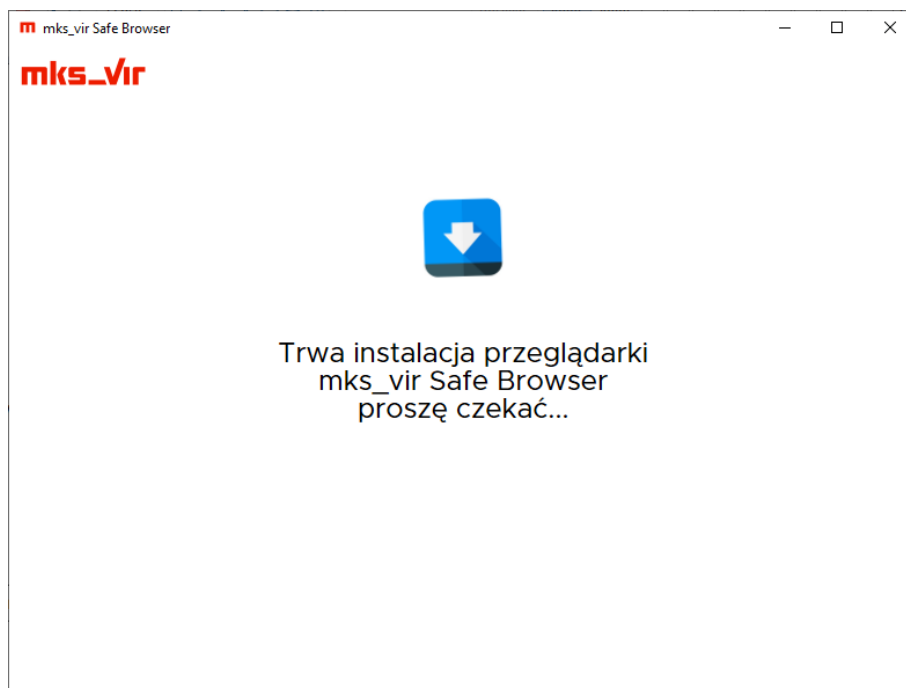
Dostęp do *bezpiecznej przeglądarki* w programie **mks_vir** jest poprzez sekcję „Narzędzia → Bezpieczna przeglądarka” w głównym oknie:



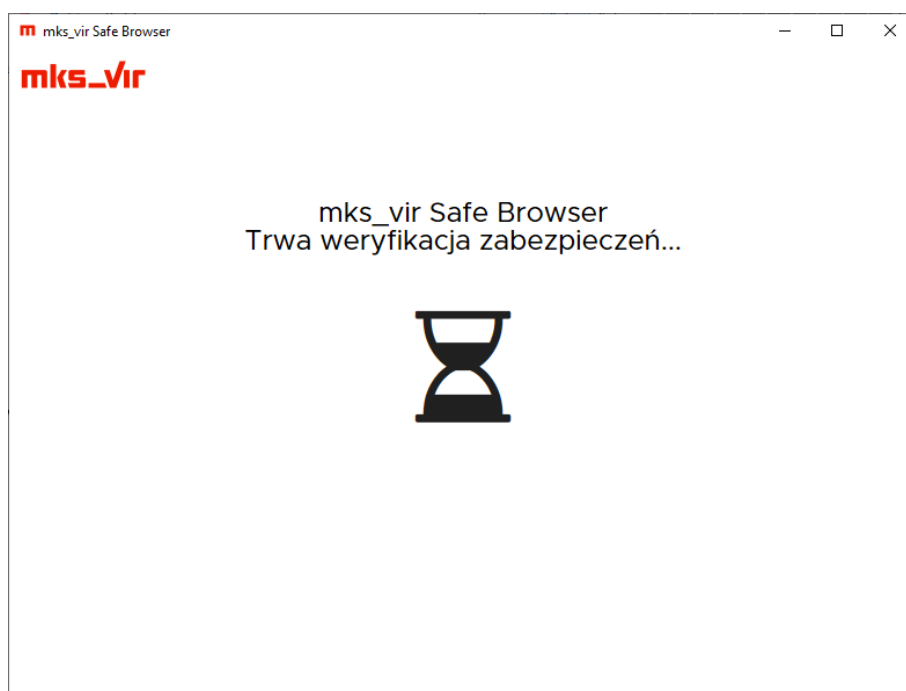
W przypadku, gdy *bezpieczna przeglądarka* nigdy jeszcze nie była użyta, po wybraniu „Bezpiecznej przeglądarki” pojawi się okno pozwalające na rozpoczęcie jej instalacji:



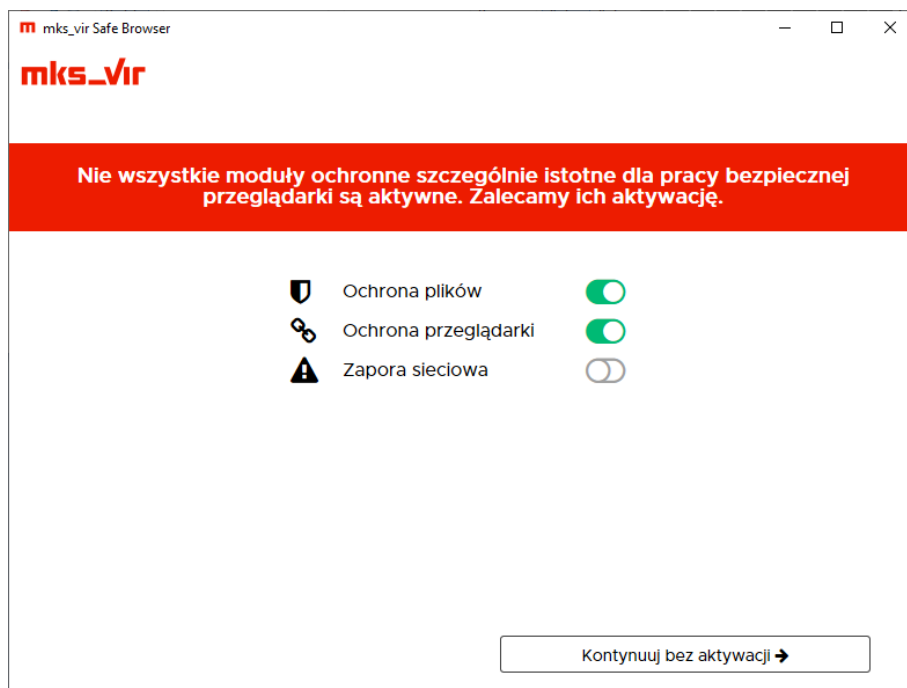
Wybranie „Tak, zainstaluj teraz przeglądarkę” rozpocznie proces instalacji:



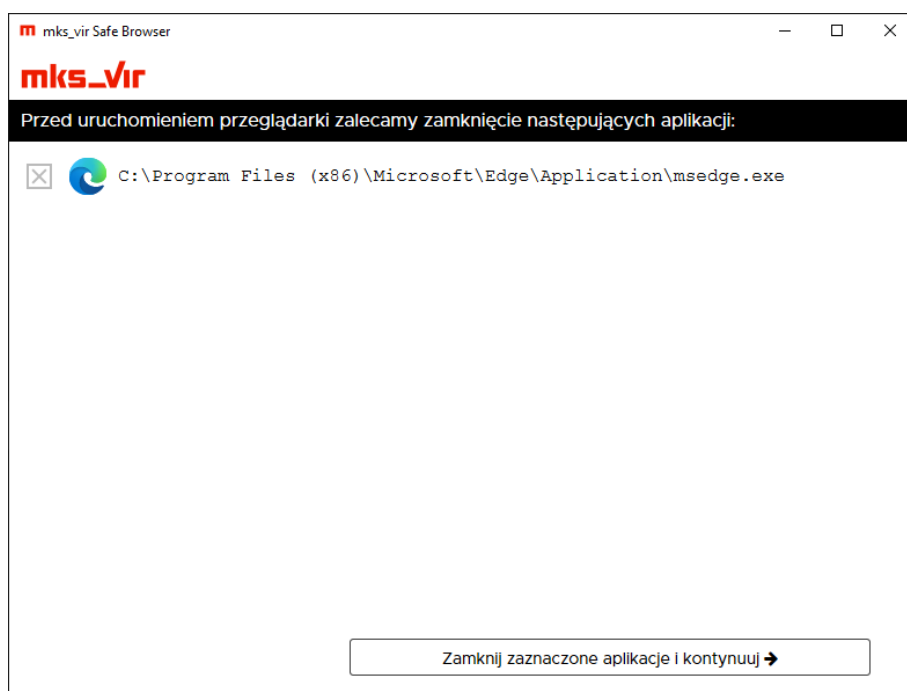
Po zakończeniu instalacji *bezpiecznej przeglądarki* lub jej uruchomieniu, jeśli już wcześniej została zainstalowana, pojawi się okno weryfikujące zabezpieczenia:



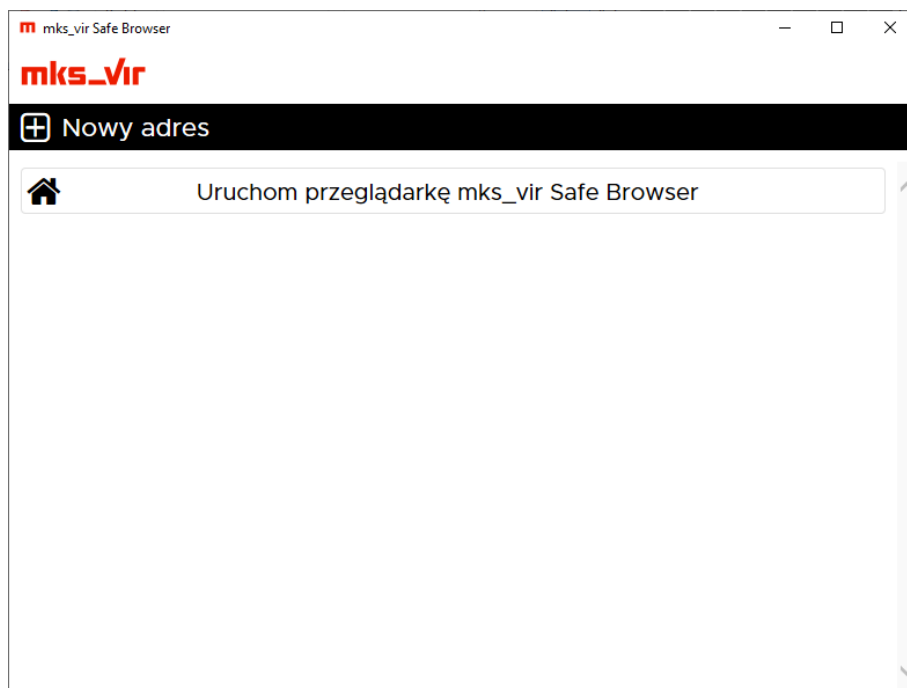
Jeśli z jakiegoś powodu wyłączony (nieaktywny) jest przynajmniej jeden z istotnych dla ochrony *bezpiecznej przeglądarki* modułów ochronnych w programie **mks_vir**, to pojawi się okno ostrzegające o tym i pozwalające na aktywację tego modułu lub kontynuowanie bez jego aktywacji:



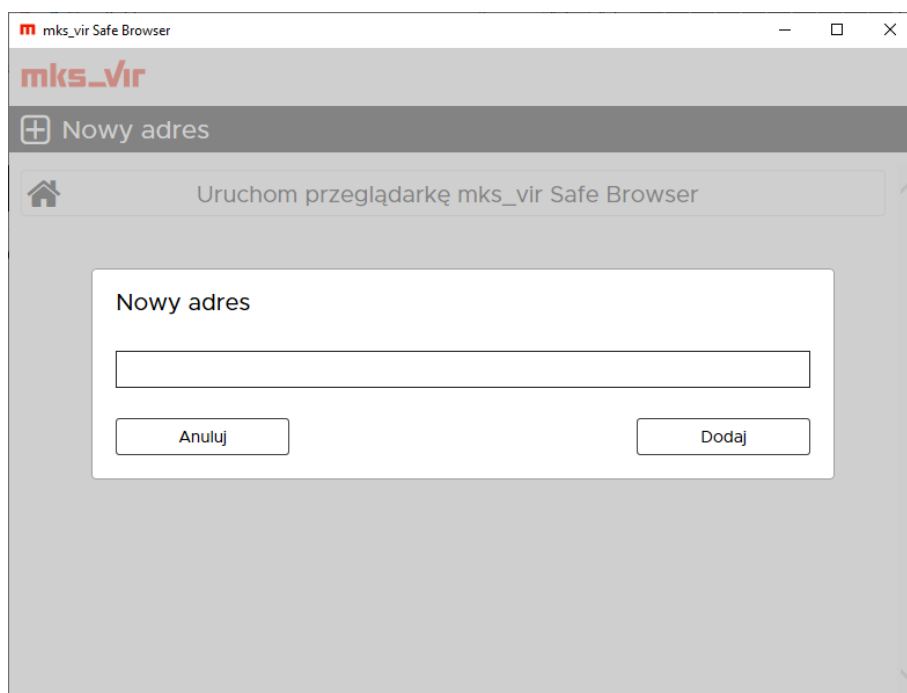
W kolejnym kroku może pojawić się okno informujące o aplikacjach stanowiących potencjalne zagrożenie bezpieczeństwa danych podawanych przez użytkownika w *bezpiecznej przeglądarce*, dlatego zalecane jest zamknięcie takich aplikacji (takie aplikacje to przede wszystkim różne przeglądarki internetowe oraz programy do zdalnego dostępu):



Po wybraniu „Zamknij zaznaczone aplikacje i kontynuuj” pojawi się okno pozwalające na uruchomienie właściwej przeglądarki oraz na zdefiniowanie najczęściej wykorzystywanych adresów stron www:

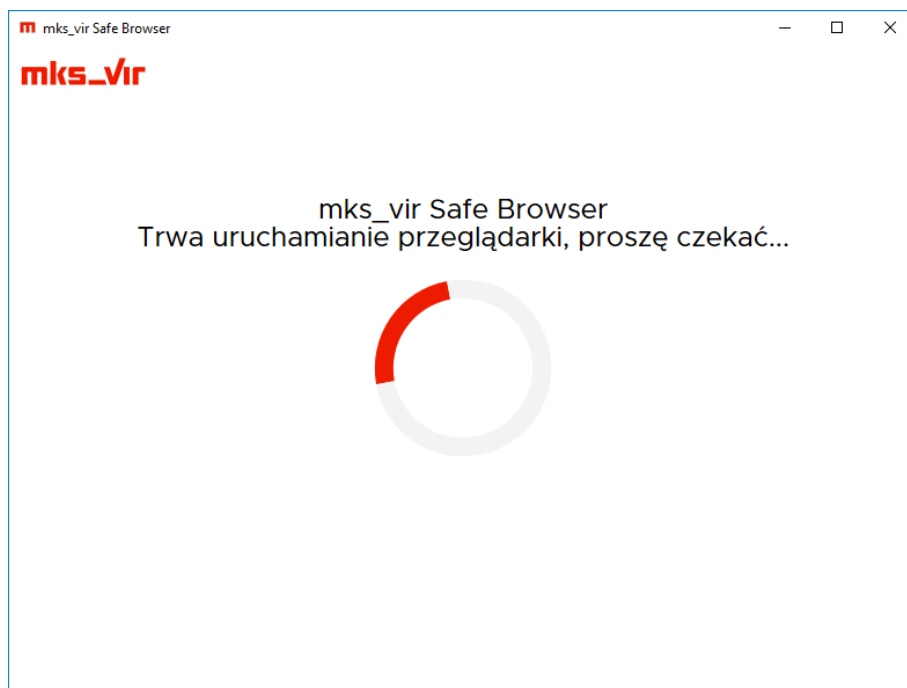


Po wybraniu opcji „Nowy adres” można wpisać adres strony do zapamiętania w programie, przy kolejnym uruchomieniu *bezpiecznej przeglądarki* wystarczy kliknąć w tak zdefiniowany adres, by strona automatycznie się otworzyła:



Uwaga! Wpisywać należy pełne adresy stron www, np. *www.adresbanku.pl*.

Wybranie opcji „Uruchom przeglądarkę mks_vir Safe Browser” spowoduje uruchomienie przeglądarki, ten proces może potrwać jakiś czas ze względu na ponowną weryfikację zabezpieczeń przez program **mks_vir**:



Po zakończeniu pojawi się właściwe okno *bezpiecznej przeglądarki*:



U góry okna przeglądarki widoczne są:

- ⏪ – przejście do poprzedniej strony
- ⏩ – przejście do następnej strony (to w przypadku, gdy wcześniej przechodziliśmy do strony poprzedniej)
- 🔄 – odświeżenie (przeładowanie) wyświetlanej strony
- 🔒 – weryfikacja certyfikatu wyświetlanej strony:
 - 🟢 – certyfikat jest prawidłowy i ważny
 - 🔴 – certyfikat jest nieprawidłowy lub nieważny

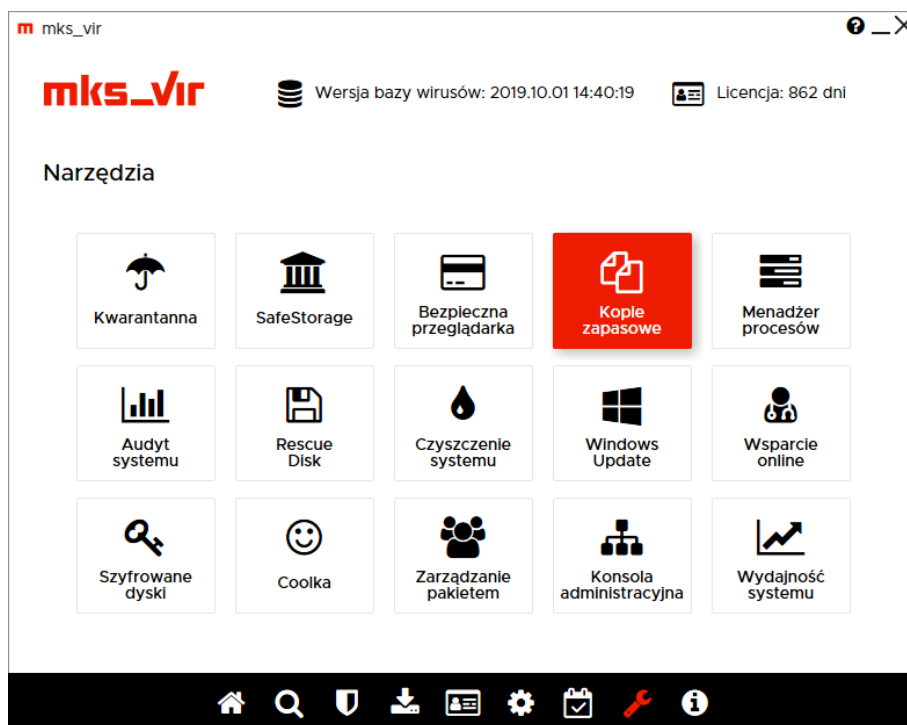
Uwaga! Pole adresowe *bezpiecznej przeglądarki* nie jest wyszukiwarką, należy tam wpisywać pełne adresy otwieranych stron www. Np. wpisanie słowa *google* spowoduje pojawienie się komunikatu z błędem, aby otworzyć tę stronę należy wpisać *google.com* lub *google.pl*.

Bezpieczna przeglądarka pozwala na jednoczesne otwieranie wielu witryn w wielu oknach, przy czym pasek adresowy stanowi dodatkowe, oddzielne okno.

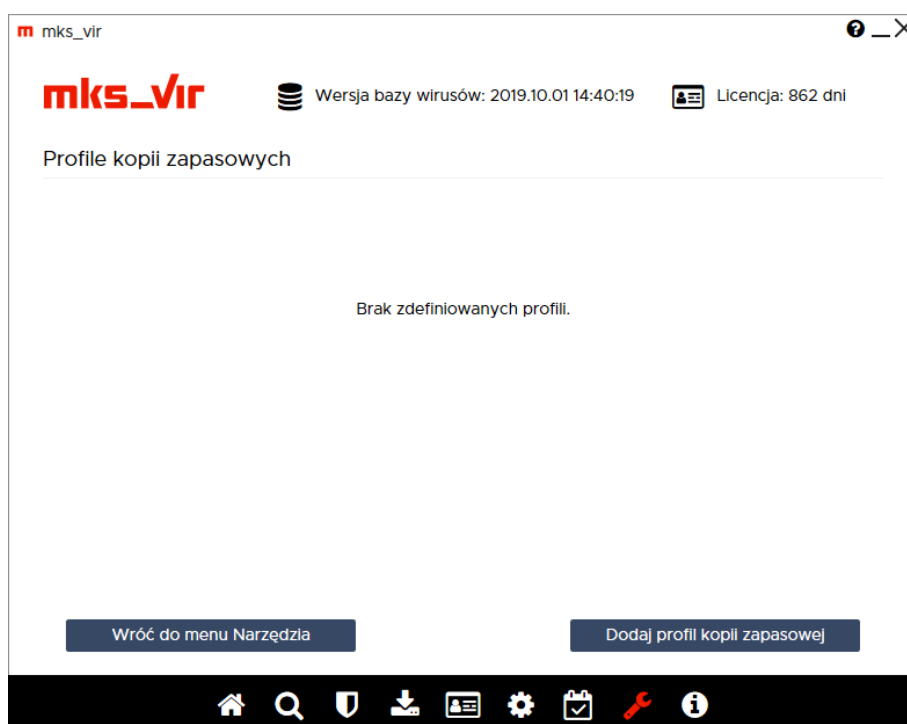
Korzystanie z kopii zapasowych (backup)

Kopia zapasowa w programie **mks_vir** pozwala na automatyczne tworzenie kopii zapasowych wskazanych przez użytkownika plików i folderów zgodnie ze zdefiniowanym harmonogramem. Oferuje predefiniowane zestawy typów plików (dokumenty, pliki graficzne, pliki audio itp.). Oferuje możliwość tworzenia kopii pełnych lub przyrostowych.

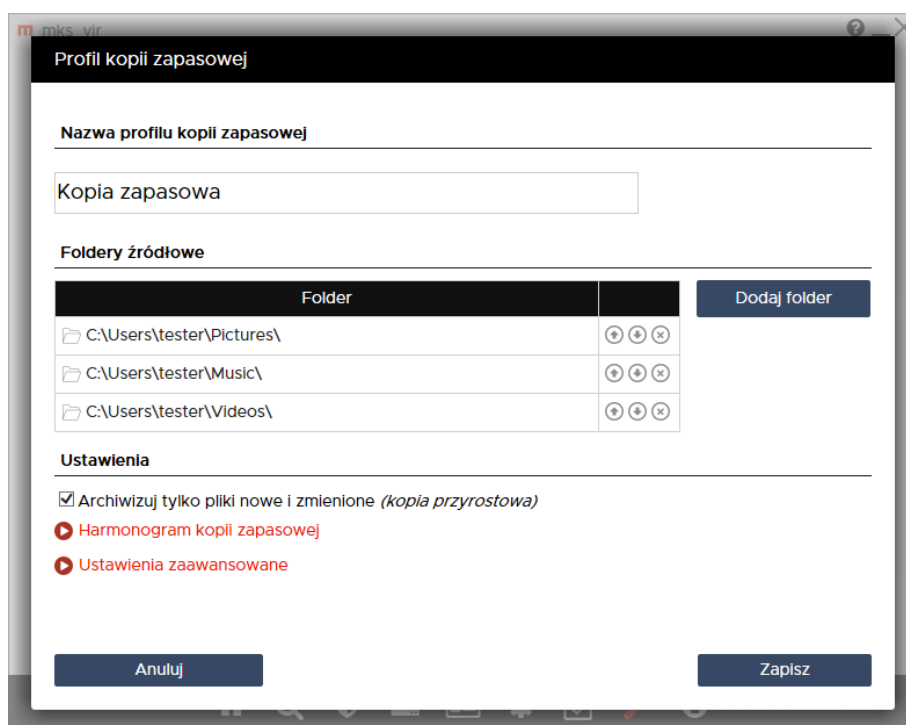
Dostęp do *kopii zapasowych (backup)* w programie **mks_vir** jest poprzez sekcję „Narzędzia → Kopie zapasowe” w głównym oknie:



Po wybraniu „Kopii zapasowych” pojawia się okno, gdzie można definiować profile dla własnych kopii zapasowych; profili takich może być wiele, a każdy może archiwizować inne dane:

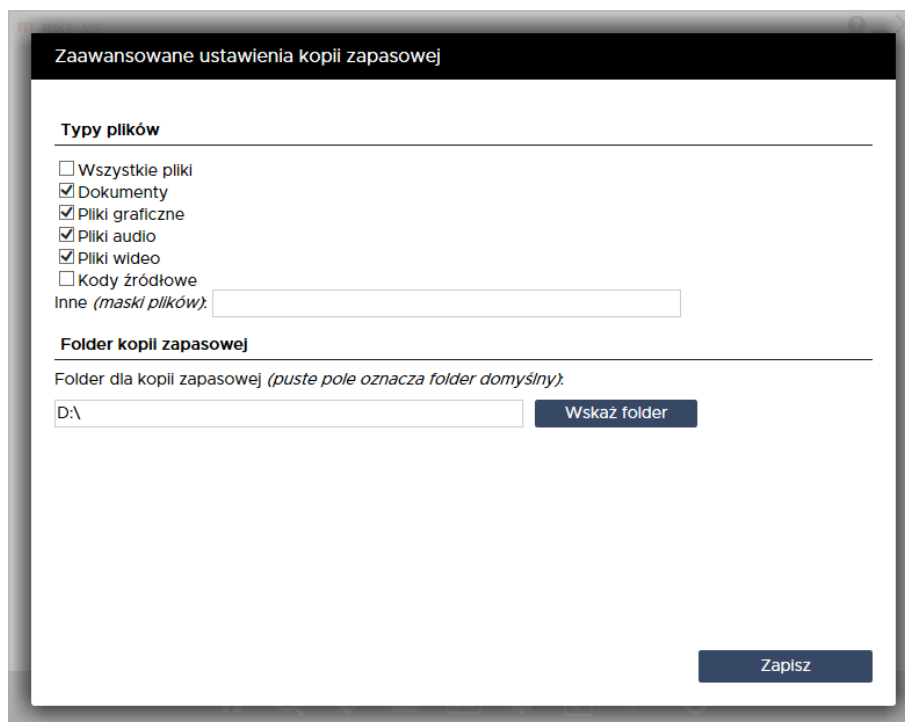


Wciśnięcie „Dodaj profil kopii zapasowej” otwiera okno pozwalające na szczegółową konfigurację danego profilu kopii zapasowej:



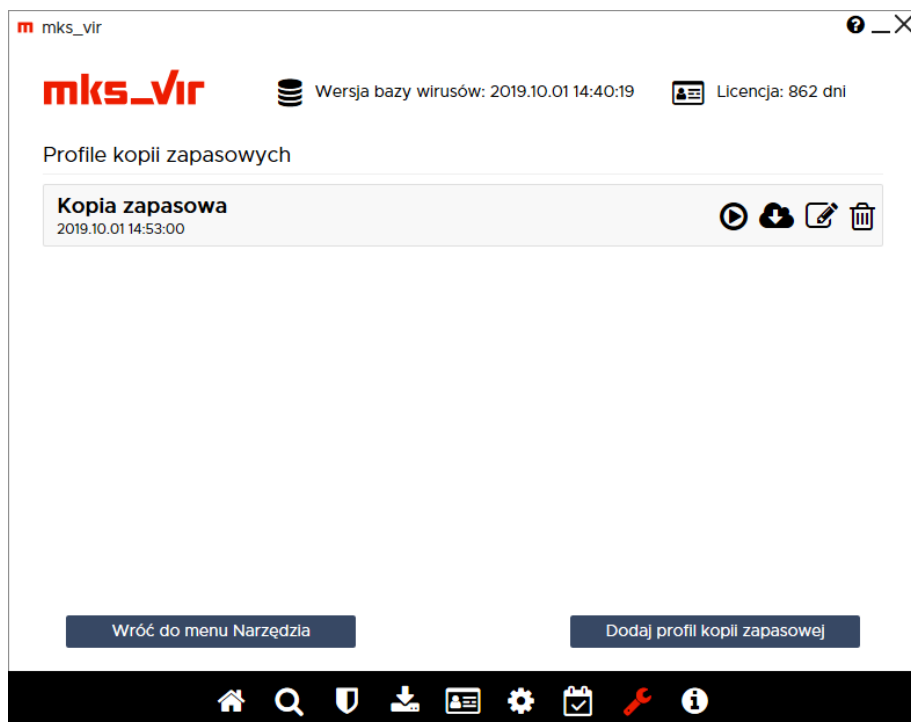
Definiując profil kopii zapasowej wypełniamy pola:

- **Nazwa profilu kopii zapasowej** – nazwa, pod którą będzie widoczny dany profil na liście profili kopii zapasowych (w przykładzie jest to „Kopia zapasowa”)
- **Foldery źródłowe** – foldery, których zawartość będzie archiwizowana w danej kopii zapasowej (w przykładzie są to foldery muzyki, filmów i zdjęć/obrazów użytkownika)
- **Ustawienia** – konfiguracja typu profilu kopii zapasowej oraz ew. terminów automatycznego wykonywania:
 - **Archiwizuj tylko pliki nowe i zmienione (kopia przyrostowa)** – włączenie tej opcji powoduje, że archiwizowane będą tylko nowe lub zmienione pliki znajdujące się w folderach źródłowych; wyłączenie tej opcji powoduje, że archiwizowane będą zawsze wszystkie pliki znajdujące się w folderach źródłowych
 - **Harmonogram kopii zapasowej** – pozwala na zdefiniowanie kiedy ma się automatycznie wykonywać archiwizacja danych za pomocą danego profilu kopii zapasowej
 - **Ustawienia zaawansowane** – otwiera „Zaawansowane ustawienia kopii zapasowej”, czyli szczegółową konfigurację profilu kopii zapasowej:



- * **Typy plików** – rodzaje danych, które mają być archiwizowane w danej kopii zapasowej:
 - **Wszystkie pliki** – archiwizowanie wszystkich rodzajów danych znajdujących się w folderach źródłowych
 - **Dokumenty** – archiwizowanie plików dokumentów (pliki tekstowe/dokumentów, arkusze kalkulacyjne, prezentacje itp.) znajdujących się w folderach źródłowych
 - **Pliki graficzne** – archiwizowanie plików zdjęć/obrazów znajdujących się w folderach źródłowych
 - **Pliki audio** – archiwizowanie plików muzycznych znajdujących się w folderach źródłowych
 - **Pliki wideo** – archiwizowanie plików filmowych znajdujących się w folderach źródłowych
 - **Kody źródłowe** – archiwizowanie plików kodów źródłowych (plików źródłowych języków programowania C/C++, Pascal, Java, JavaScript itp.) znajdujących się w folderach źródłowych
 - **Inne (*maski plików*)** – definowanie własnych kryteriów doboru danych do archiwizacji znajdujących się w folderach źródłowych
- * **Folder kopii zapasowej:**
 - **Folder dla kopii zapasowej (*puste pole oznacza folder domyślny mks_vir*)** – folder docelowy, gdzie tworzone i aktualizowane będzie archiwum danej kopii zapasowej; zalecane jest, by wskazywać tu inną lokalizację (dysk, zasób sieciowy) niż te, na których znajdują się foldery źródłowe

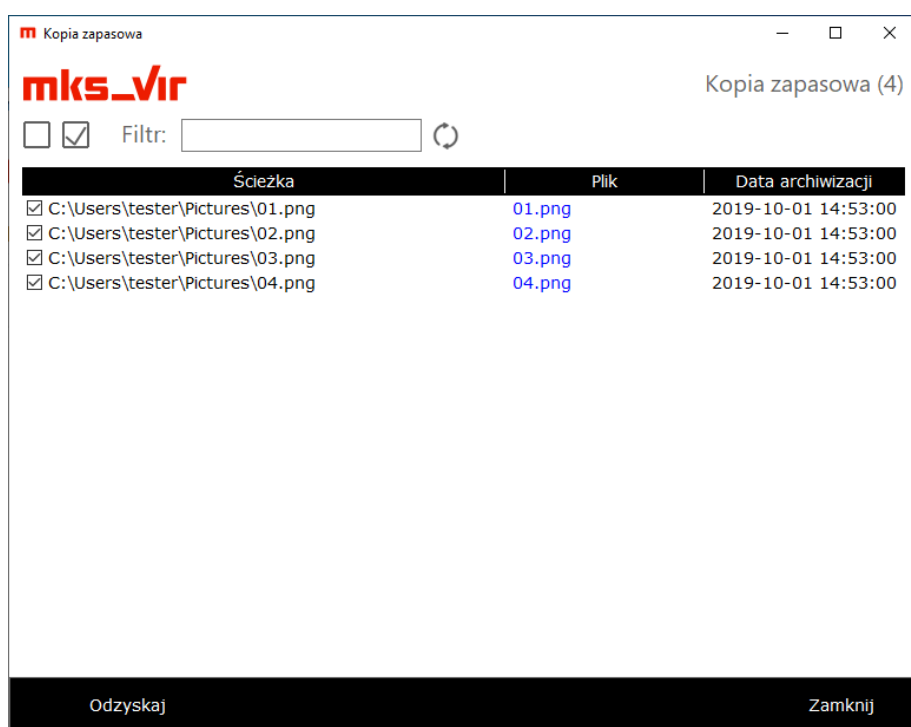
Wybranie „Zapisz” zapisuje ustawione parametry profilu kopii zapasowej i zamyka okno konfiguracji:



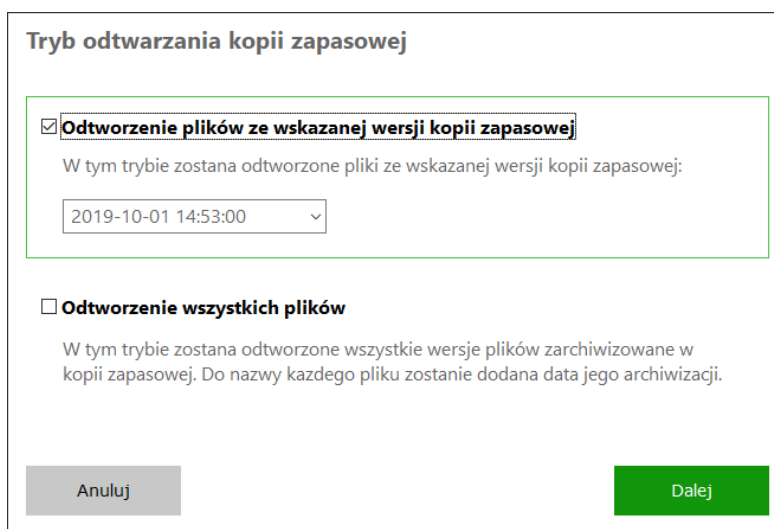
Poszczególne ikony widoczne przy danym profilu kopii:

- – wymusza uruchomienie archiwizowania danych w kopii zapasowej
- – pozwala na odzyskanie danych z kopii zapasowej
- – umożliwia modyfikację parametrów profilu kopii zapasowej
- – usuwa profil kopii zapasowej

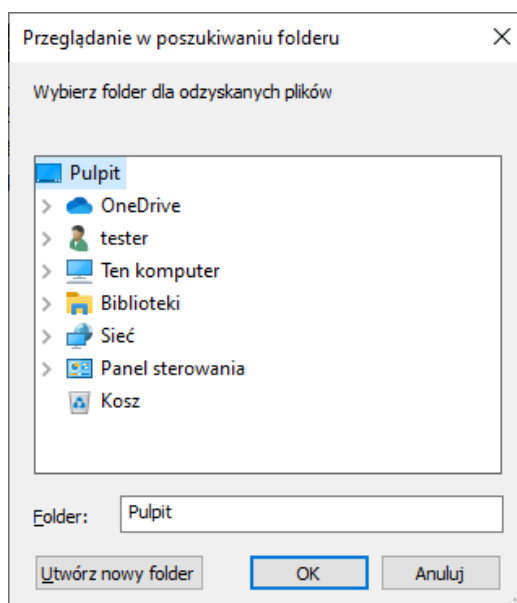
Wybranie skutkuje wyświetleniem okna z zawartością archiwum danej kopii zapasowej:



Po zaznaczeniu plików do odzyskania i wybraniu „Odzyskaj” pojawia się okno umożliwiające wybór, z której wersji kopii zapasowej chcemy odzyskać pliki (do wyboru jest albo konkretny termin, albo wszystkie pliki; w przykładzie wybieramy konkretny termin wykonania kopii zapasowej):

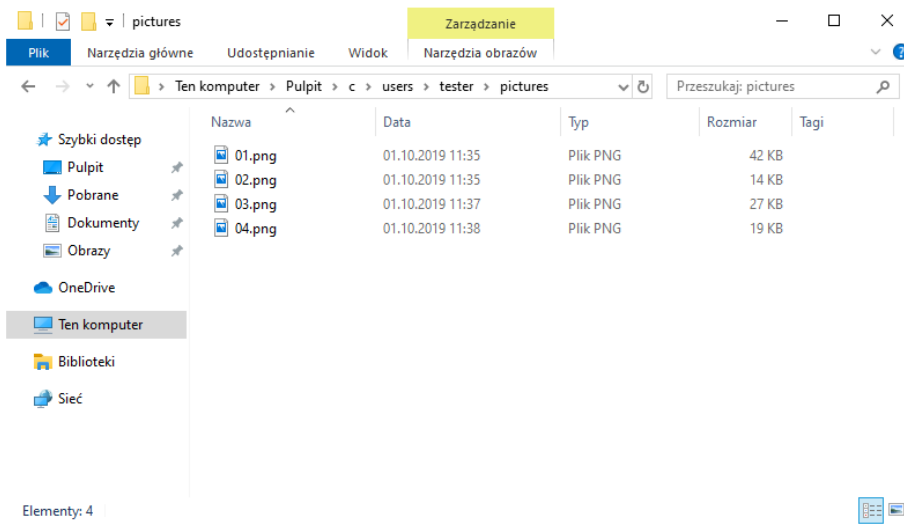


Po wybraniu „Dalej” pojawia się okno pozwalające na wybór lokalizacji, gdzie zostaną odzyskane pliki z archiwum kopii zapasowej (w przykładzie jest to pulpit):



Wybranie „OK” rozpocznie proces odzyskiwania plików. Po zakończeniu odzyskiwania można otworzyć folder, gdzie znajdują się tak odzyskane pliki; przy odzyskiwaniu odtwarzana jest struktura katalogów, z których pochodziły odtwarzane pliki, dlatego w przykładzie podfolder, gdzie znajdują się odtworzone pliki to:

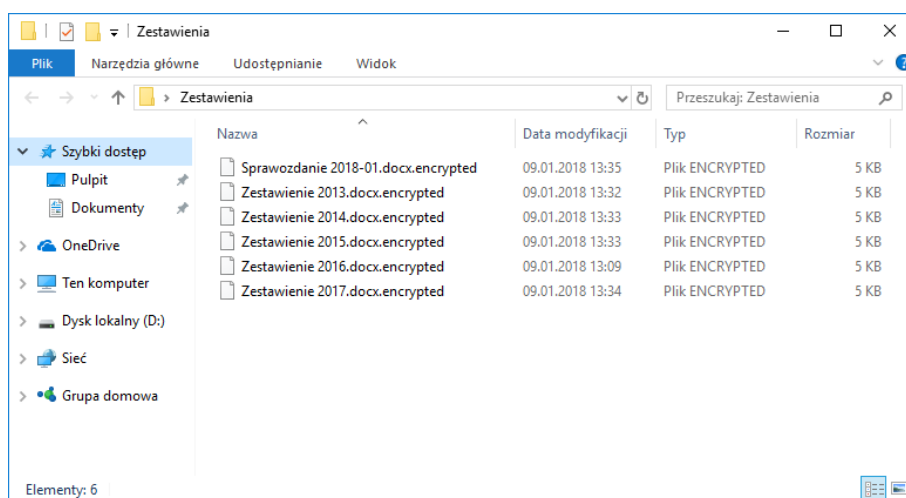
```
c:\users\tester\pictures
```



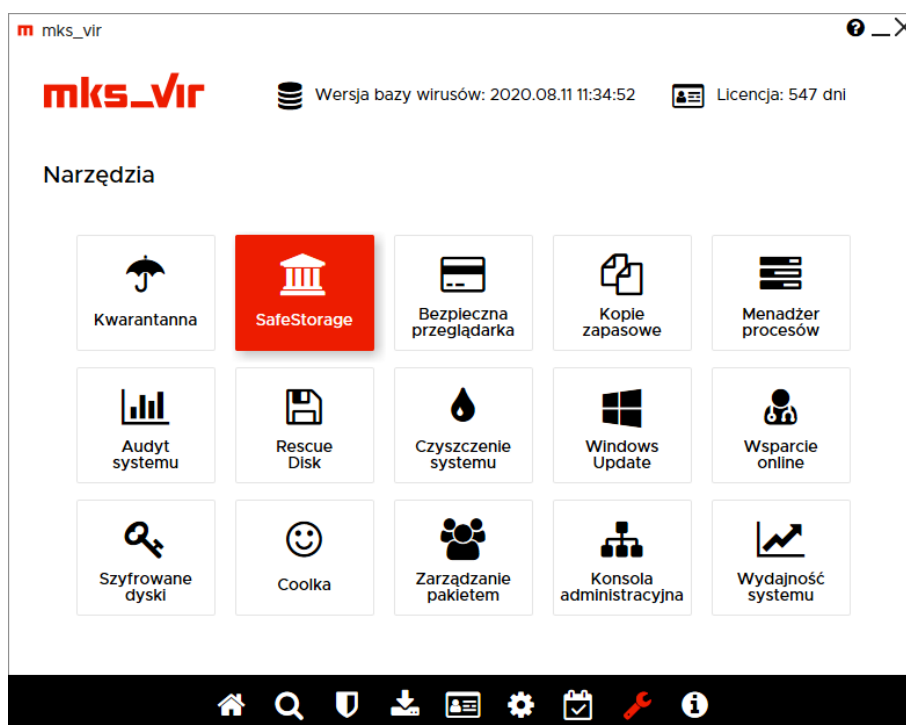
Odzyskiwanie danych za pomocą SafeStorage

Wbudowany w program **mks_vir** mechanizm **SafeStorage** to nowatorska technologia pozwalająca na ochronę ważnych danych (różnego rodzaju dokumentów, plików graficznych, baz, arkuszy, prezentacji itp.) przed ich niepożądaną modyfikacją, zaszyfrowaniem, zniszczeniem lub skasowaniem przez szkodliwe oprogramowanie (np. przez zagrożenia z rodzin *Cryptolocker*, *CTB-Locker*, *TeslaCrypt* itp.), jak również przez przypadkowe działanie użytkownika

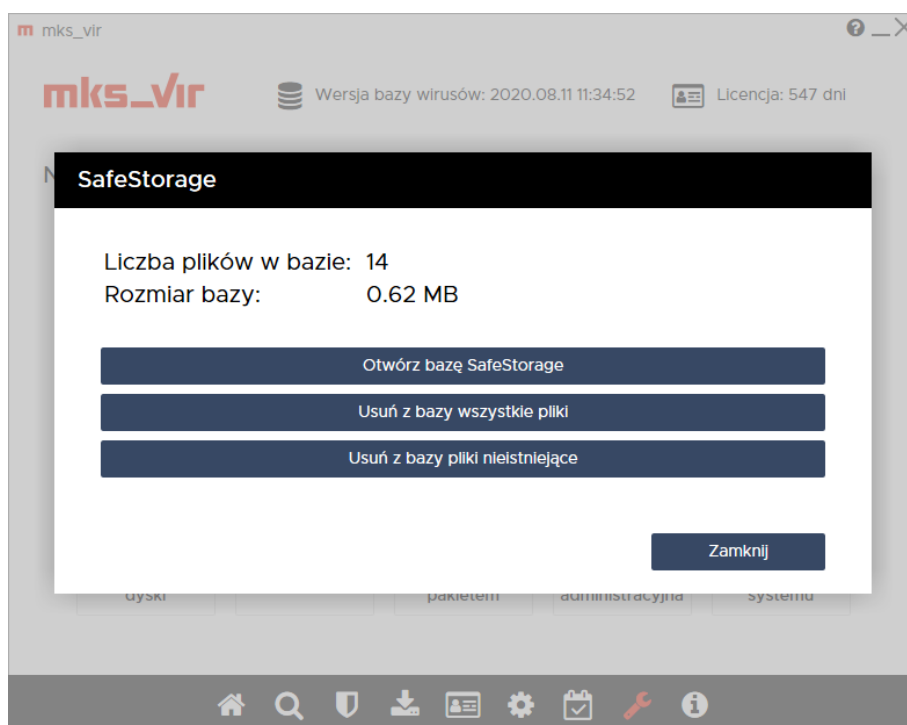
Na poniższym obrazku widać folder z zaszyfrowanymi po ataku *Cryptolockera* plikami. Po takim ataku sama zmiana nazwy nie wystarczy (w tym przypadku byłoby to usunięcie rozszerzenia „encrypted”), zawartość plików nadal nie będzie dostępna



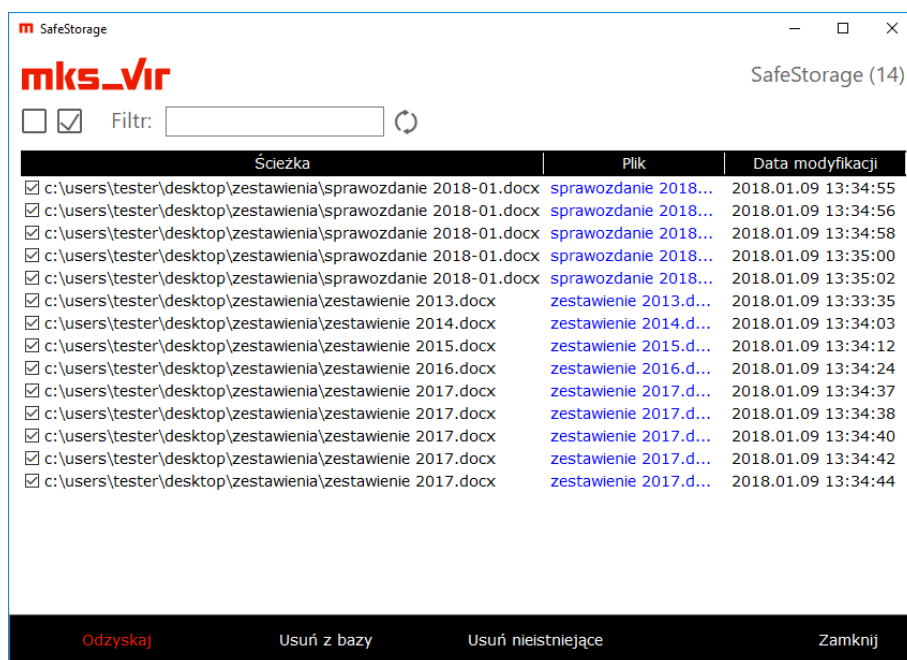
Właśnie dla ochrony danych w takich przypadkach został wprowadzony mechanizm **SafeStorage**. Dostęp do niego znajdziemy w głównym oknie programu **mks_vir**, w sekcji „Narzędzia”:



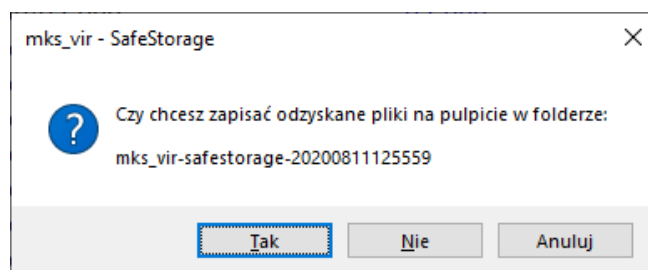
Po wybraniu „SafeStorage” pojawi się okno, w którym wybieramy „Otwórz bazę SafeStorage”:



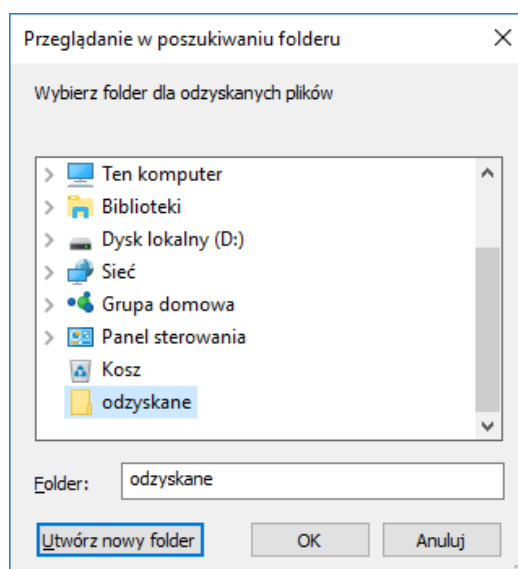
co otworzy narzędzie do zarządzania zawartością *SafeStorage* – znajdziemy tam pliki, które możemy odtworzyć. Mechanizm ten przechowuje kilka ostatnich wersji plików, dzięki czemu możemy go wykorzystać również w celu odtworzenia plików do wersji sprzed zmian, które już po ich wprowadzeniu użytkownik mógłby uznać za niepotrzebne lub błędne



Po wybraniu plików, które zamierzamy odtworzyć (w przykładzie powyżej są to wszystkie pliki) wybieramy przycisk „Odzyskaj”. Program domyślnie proponuje zapisanie odzyskiwanych plików do folderu na pulpicie:

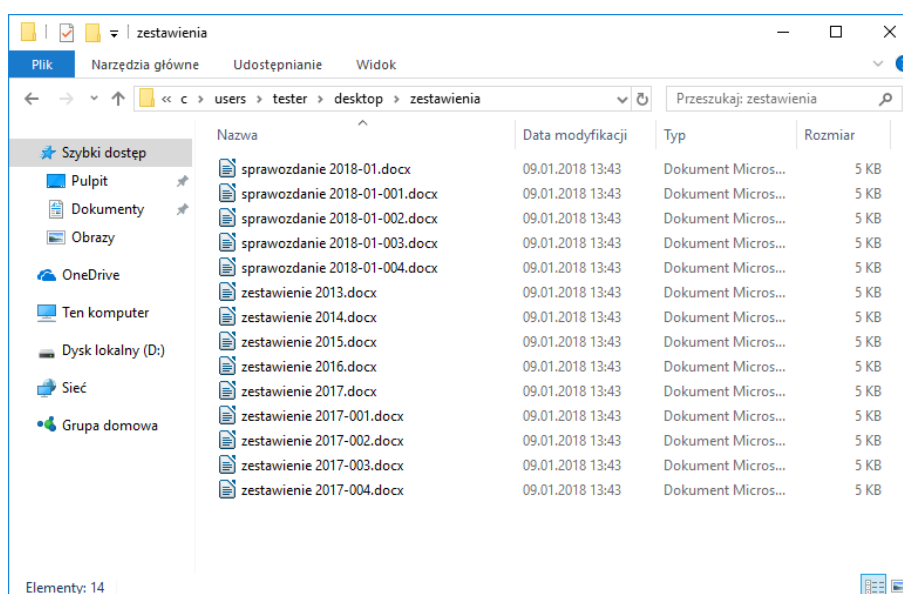


Po wybraniu „Tak” pliki zostaną odzyskane do tego właśnie folderu. Po wybraniu „Nie” pojawi się standardowe okno wyboru folderu, gdzie pliki mają zostać odzyskane. Wciśnięcie „OK” rozpocznie odzyskiwanie plików



Po zakończeniu odzyskiwania można otworzyć folder, gdzie znajdują się tak odzyskane pliki; przy odzyskiwaniu odtwarzana jest struktura katalogów, z których pochodziły odtwarzane pliki, dlatego w przykładzie podfolder, gdzie znajdują się odtworzone pliki to:

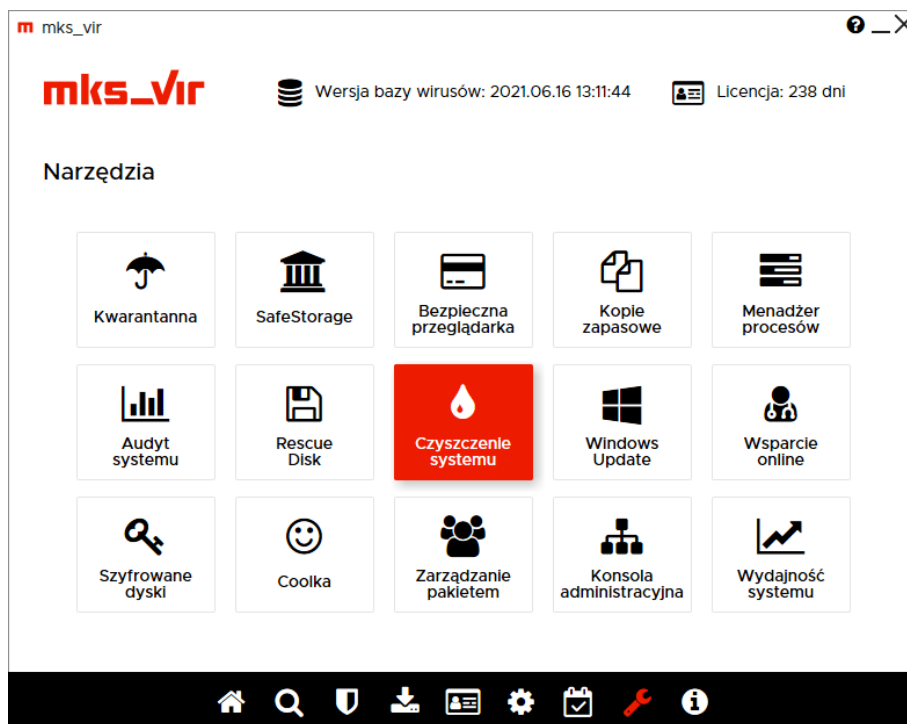
c:\users\tester\desktop\zestawienia



Teraz wystarczy odtworzone pliki przejrzeć, pozostawiając tylko te, które są rzeczywiście potrzebne

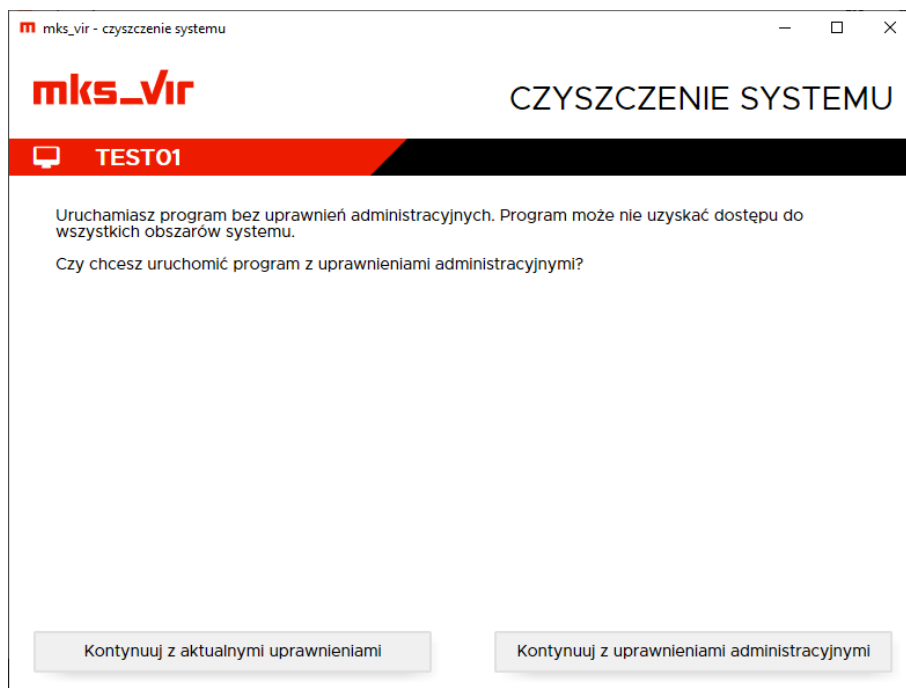
Korzystanie z modułu czyszczenia systemu

Program **mks_vir** posiada narzędzie, które umożliwia szybką analizę i usunięcie niepotrzebnych obiektów zaśmiecających dyski komputera. Tym narzędziem jest moduł „Czyszczenie systemu”, a dostęp do niego znajdziemy w głównym oknie programu **mks_vir**, w sekcji „Narzędzia”:



Po wybraniu „Czyszczenia systemu” pojawi się okno, w którym możemy wybrać tryb uruchomienia modułu:

- **Kontynuuj z aktualnymi uprawnieniami** – uruchamia moduł „Czyszczenia systemu” z uprawnieniami aktualnie zalogowanego użytkownika, przez co będzie możliwe wyczyszczenie tylko folderów, do których ma dostęp użytkownik – w większości przypadków są to foldery tymczasowe użytkownika i dane przeglądarek
- **Kontynuuj z uprawnieniami administracyjnymi** – uruchamia moduł „Czyszczenia systemu” z uprawnieniami administracyjnymi, dzięki czemu będzie możliwe wyczyszczenie nie tylko folderów, do których ma dostęp użytkownik, ale także folderów z danymi tymczasowymi systemu



Po wybraniu jednego z trybów moduł rozpoczyna analizowanie systemu, w celu określenia obiektów, które będą możliwe do usunięcia – operacja ta zależnie od aktualnego stanu systemu może trochę potrwać:



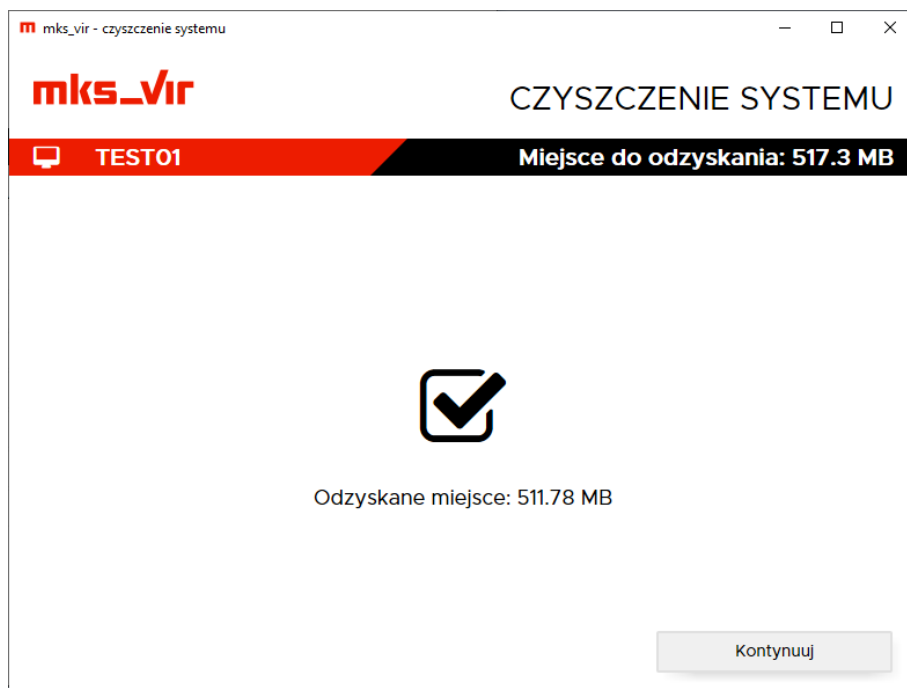
Po zakończeniu analizy wyświetla się w oknie lista kategorii obiektów, które można wyczyścić wraz z informacjami o zajmowanym przez pliki z tych kategorii miejscu na dysku – kliknięcie w daną kategorię powoduje wyłączenie czyszczenia należących do niej plików (kategoria zostaje wtedy wyszarzona), ponowne kliknięcie w taką kategorię znowu włącza ją do czyszczenia:



Wybranie „Wyczyść system” rozpoczyna usuwanie zbędnych plików – cała operacja może trochę potrwać zależnie od aktualnego stanu systemu oraz ilości zbędnych plików:



Po zakończeniu operacji czyszczenia pojawi się informacja ile miejsca zostało odzyskane w wyniku działania modułu:



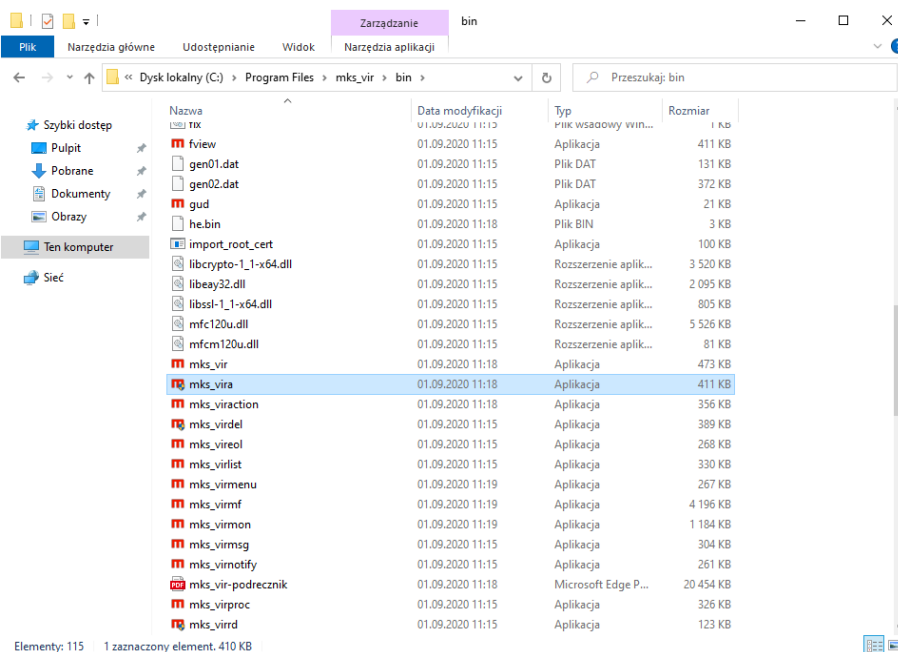
Wybranie „Kontynuuj” w okienku powyżej spowoduje powrót do okna umożliwiającego rozpoczęcie czyszczenia systemu:



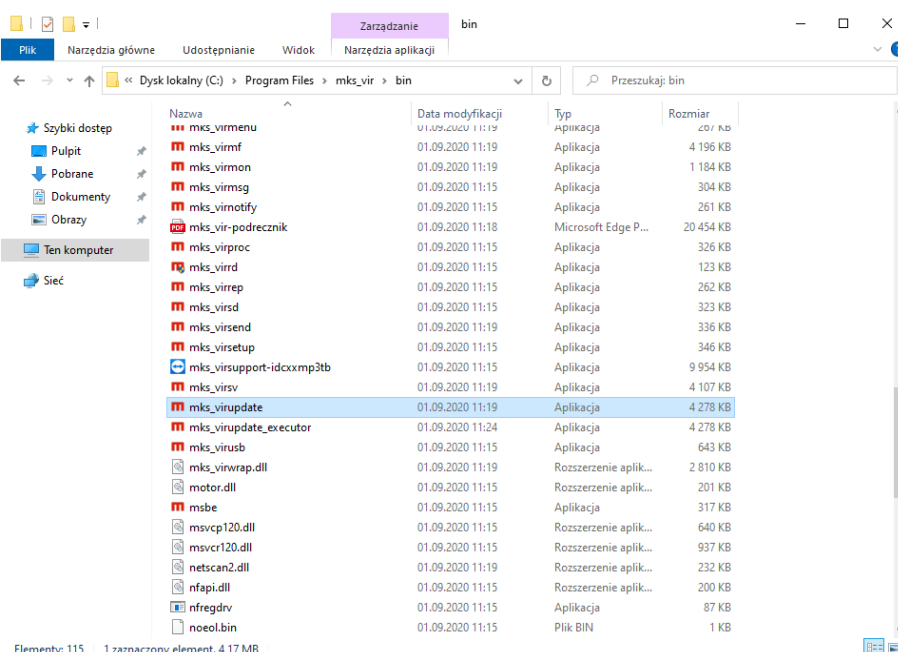
Moduł „Czyszczenia systemu” nie zawsze będzie w stanie usunąć niepotrzebne pliki, np. dlatego że będą w użyciu (otwarte) przez jakieś uruchomione programy. Ponadto w czasie działania modułu mogą pojawiać się nowe, niepotrzebne pliki, nieuwzględnione w pierwotnej analizie obiektów możliwych do usunięcia.

Skanowanie programem mks_vir w trybie awaryjnym Windows

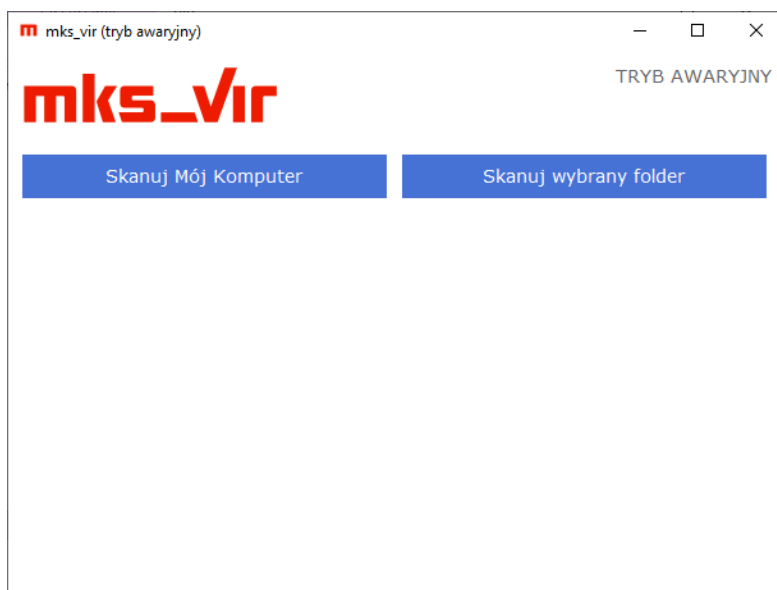
Program **mks_vir** umożliwia przeskanowanie dysków komputera nie tylko w czasie normalnej pracy systemu Windows, ale także gdy ten jest uruchomiony w trybie awaryjnym. Do skanowania w trybie awaryjnym służy specjalny skaner trybu awaryjnego „mks_vira”, znajdujący się w folderze `c:\program files\mks_vir\bin`:



Jeśli system Windows jest uruchomiony w trybie awaryjnym z obsługą sieci, to jest możliwa aktualizacja skanera trybu awaryjnego **mks_vir** za pomocą programu „mks_virupdate”, znajdującego się w folderze `c:\program files\mks_vir\bin` (wystarczy w tym celu uruchomić ten program i poczekać aż skończy działanie):

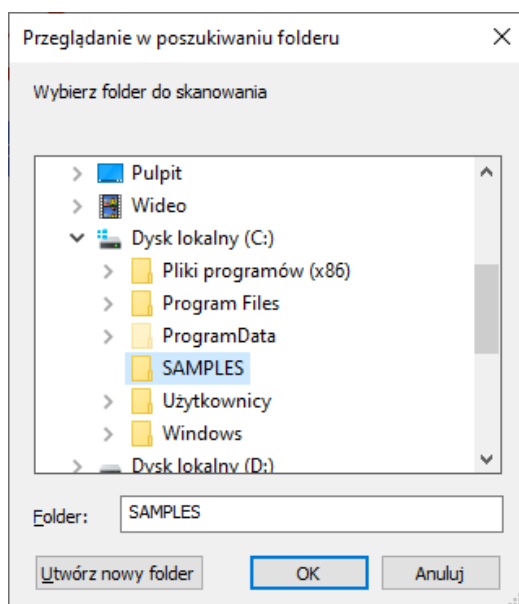


Po uruchomieniu programu „mks_vira” pojawi się jego okno, w którym można wybrać obszar skanowania:

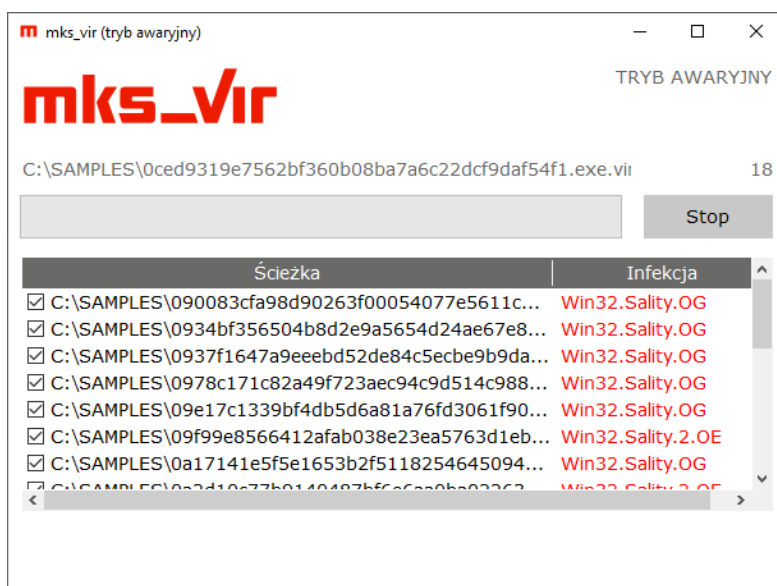


Po wybraniu *Skanuj Mój Komputer* program rozpocznie skanowanie wszystkich dostępnych w danym komputerze dysków.

W przypadku wybrania *Skanuj wybrany folder* program umożliwi wskazanie folderu do skanowania:

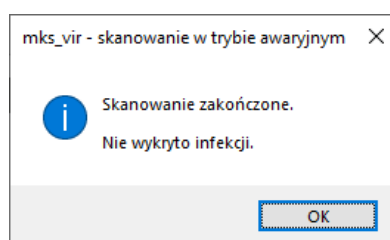


W przypadku znalezienia zagrożeń w czasie skanowania w oknie programu pojawi się lista z już wykrytymi zainfekowanymi plikami:

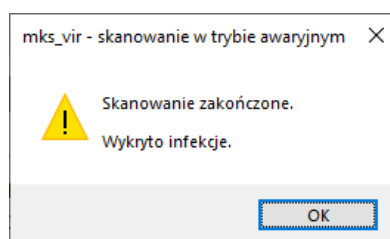


Zakończenie skanowania zostanie zasygnalizowane odpowiednim okienkiem:

- w przypadku braku infekcji:

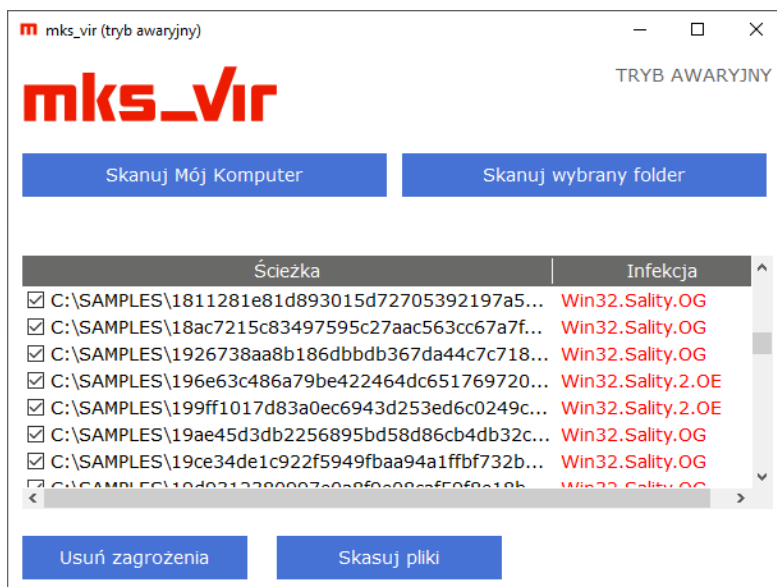


- w przypadku wykrycia infekcji:

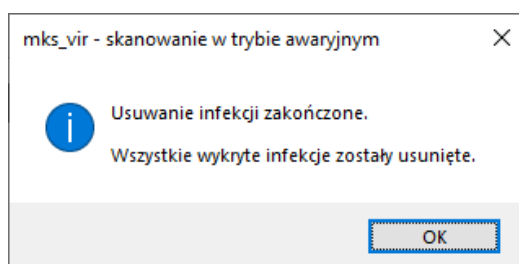


Jeśli zostały wykryte zainfekowane pliki, po zakończeniu skanowania pojawi się okno z możliwością wyboru akcji:

- **Usuń zagrożenia** - program leczy te zainfekowane pliki, które da się wyleczyć, a pozostałe zainfekowane kasuje
- **Skasuj pliki** - program kasuje wszystkie wykryte zainfekowane pliki.



Zakończenie leczenia/kasowania zainfekowanych plików zostanie zasygnalizowane odpowiednim okienkiem:

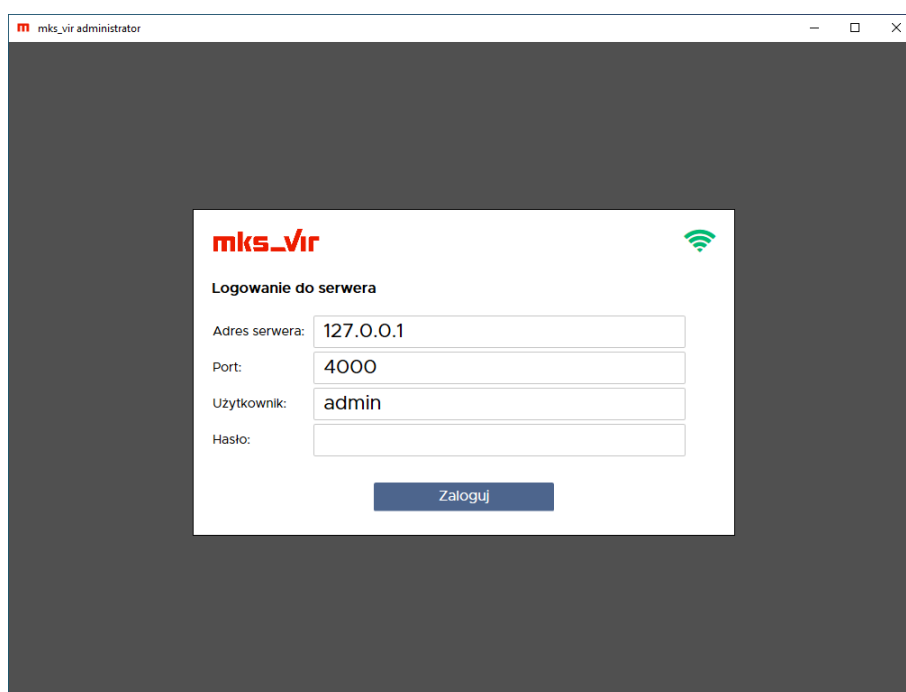


mks_vir administrator

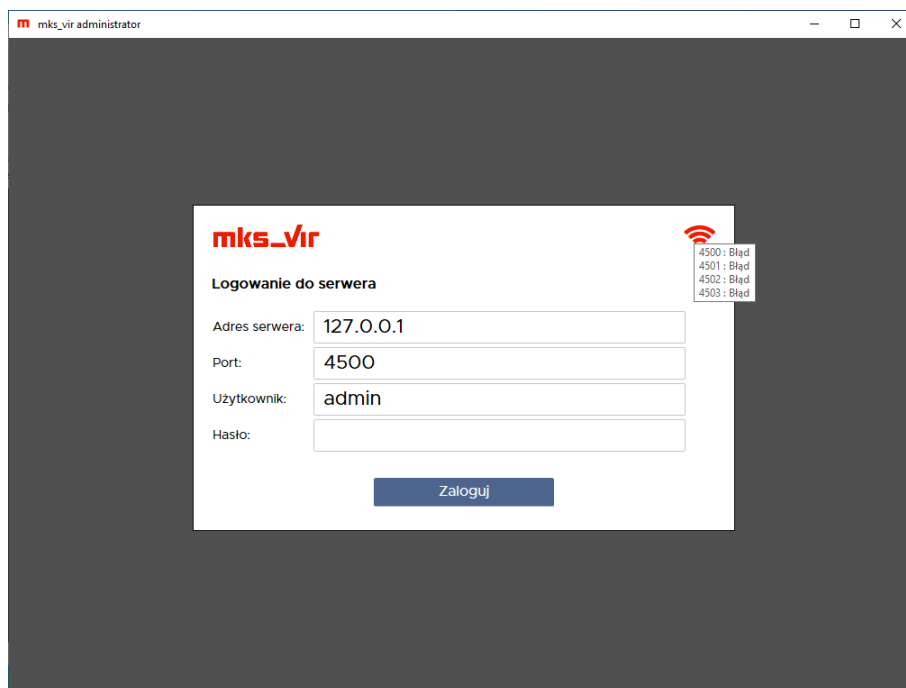
mks_vir administrator służy do zarządzania instalacjami pakietów **mks_vir** w sieci

Przed logowaniem za pomocą konsoli zarządzającej do serwera zarządzającego **mks_vir administrator** sprawdzana jest dostępność serwera zarządzającego pod wpisanym adresem za pomocą zadeklarowanych portów komunikacyjnych, co sygnalizuje kolor ikony 📶.

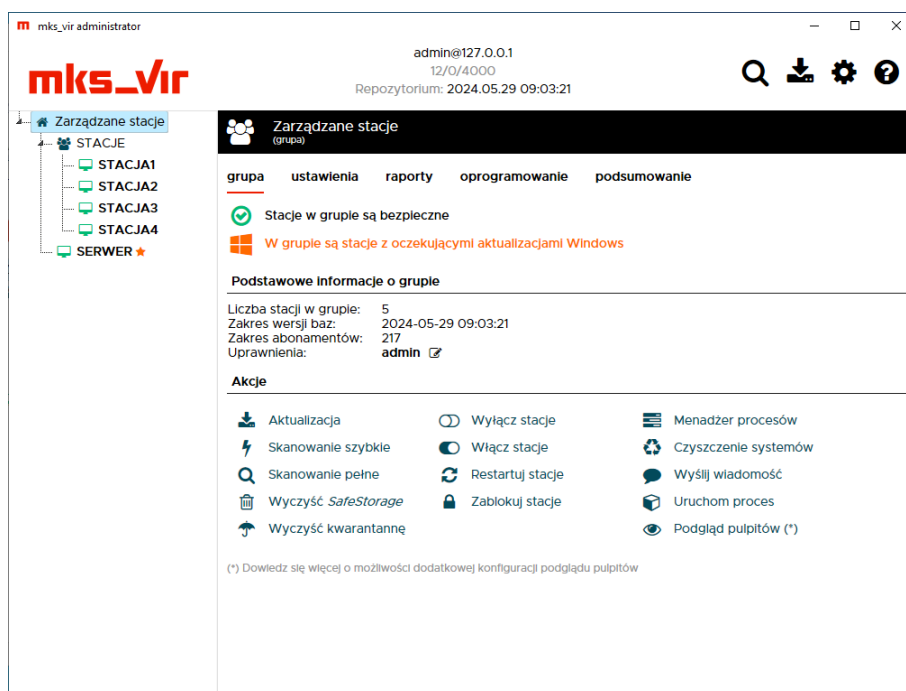
Jeśli serwer jest dostępny ikona ma kolor zielony 📶:



Jeśli serwer nie jest dostępny ikona ma kolor czerwony 📶 – najeżdżając kursorem myszy na tę ikonę można sprawdzić, które z portów nie są dostępne (są blokowane lub zajęte przez jakieś inne oprogramowanie):



Po zalogowaniu do konsoli, po lewej stronie dostępna jest lista grup i zarządzanych stacji. Po prawej stronie domyślnie widoczny jest status wybranego elementu (grupy lub stacji) oraz możliwe do wykonania na nim akcje



Jeśli jest widoczny napis „**W grupie są stacje z oczekującymi aktualizacjami Windows**”, to znaczy że na części stacji są oczekujące na instalację aktualizacje systemu Windows.


Ikony widoczne u góry okna konsoli, po prawej stronie, oznaczają:

Q – wyszukiwanie stacji w bazie serwera zarządzającego **mks_vir administrator** na podstawie wprowadzonej frazy


podanie **+** (opcjonalnie) oznacza, że dane słowo musi występować, zaś podanie **-** oznacza, że dane słowo nie może występować (np. podanie „intel-realtek” wyszuka

wszystkie stacje, w których danych występuje słowo „intel” i jednocześnie nie występuje słowo „realtek”)

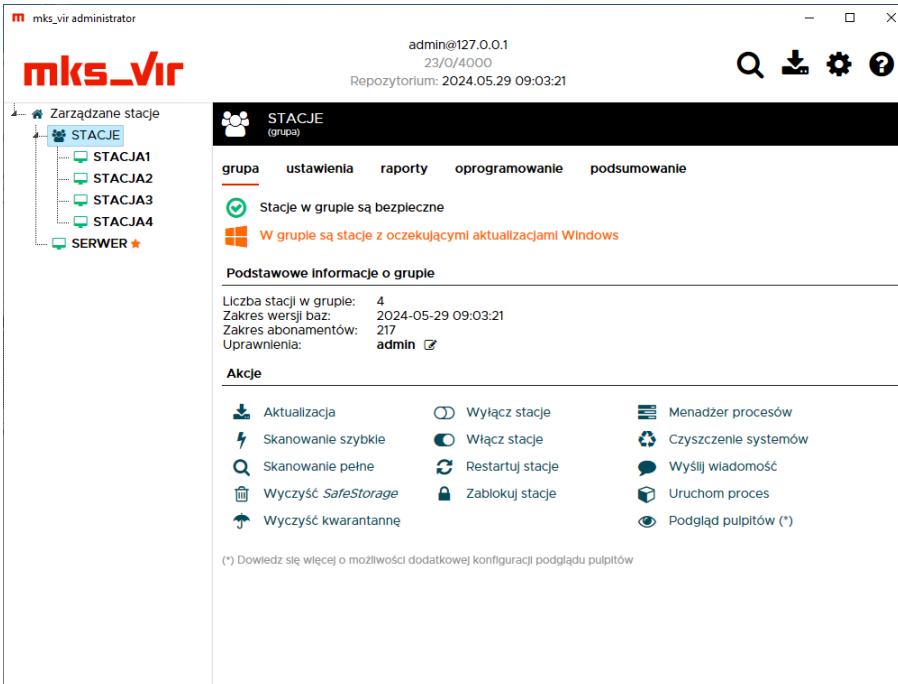
po wyszukaniu stacji ikona **Q** zmieni się w ikonę **X** – jej wciśnięcie zresetuje wyniki wyszukiwania

 – uruchomienie aktualizacji serwera zarządzającego **mks_vir administrator** oraz repozytorium aktualizacyjnego dla stacji

 – ustawienia serwera zarządzającego i konsoli **mks_vir administrator**

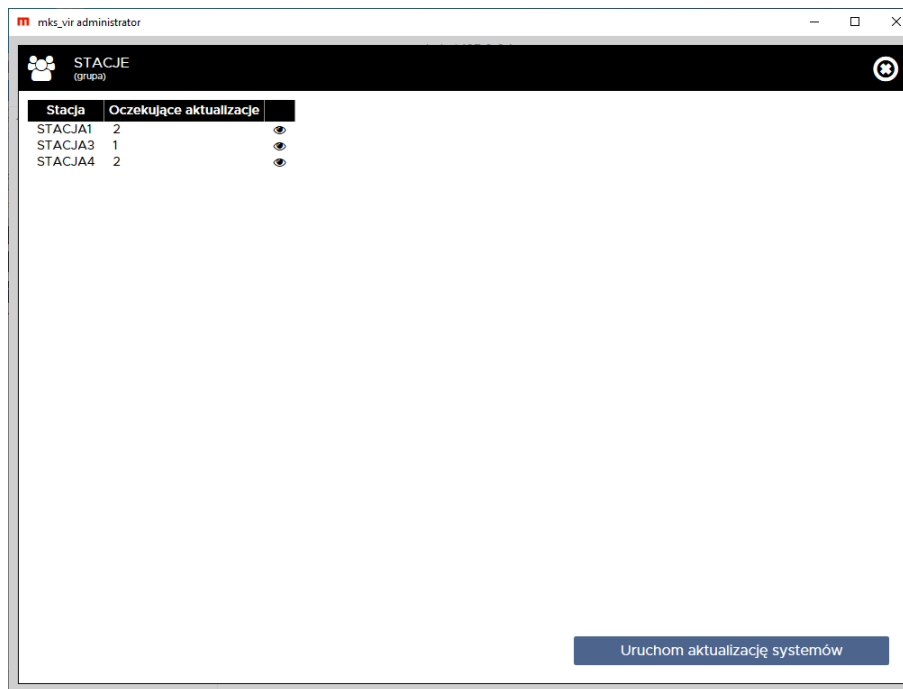
 – dostęp do podręcznika **mks_vir**


Podstawowe informacje o grupie:



The screenshot shows the 'mks_vir administrator' interface. At the top, it displays the user 'admin@127.0.0.1' with '23/0/4000' and a repository timestamp of '2024.05.29 09:03:21'. The main content area is titled 'STACJE (grupa)' and has tabs for 'grupa', 'ustawienia', 'raporty', 'oprogramowanie', and 'podsumowanie'. A green checkmark indicates 'Stacje w grupie są bezpieczne', but an orange warning icon states 'W grupie są stacje z oczekującymi aktualizacjami Windows'. Below this, 'Podstawowe informacje o grupie' lists: 'Liczba stacji w grupie: 4', 'Zakres wersji baz: 2024-05-29 09:03:21', 'Zakres abonamentów: 217', and 'Uprawnienia: admin'. An 'Akcje' section contains a grid of icons for actions such as 'Aktualizacja', 'Skanowanie szybkie', 'Skanowanie pełne', 'Wyczyść SafeStorage', 'Wyczyść kwarantannę', 'Wyłącz stacje', 'Włącz stacje', 'Restartuj stacje', 'Zablokuj stacje', 'Menadżer procesów', 'Czyszczenie systemów', 'Wyślij wiadomość', 'Uruchom proces', and 'Podgląd pulpitów (*)'. A footnote at the bottom says '(*) Dowiedz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitów'.

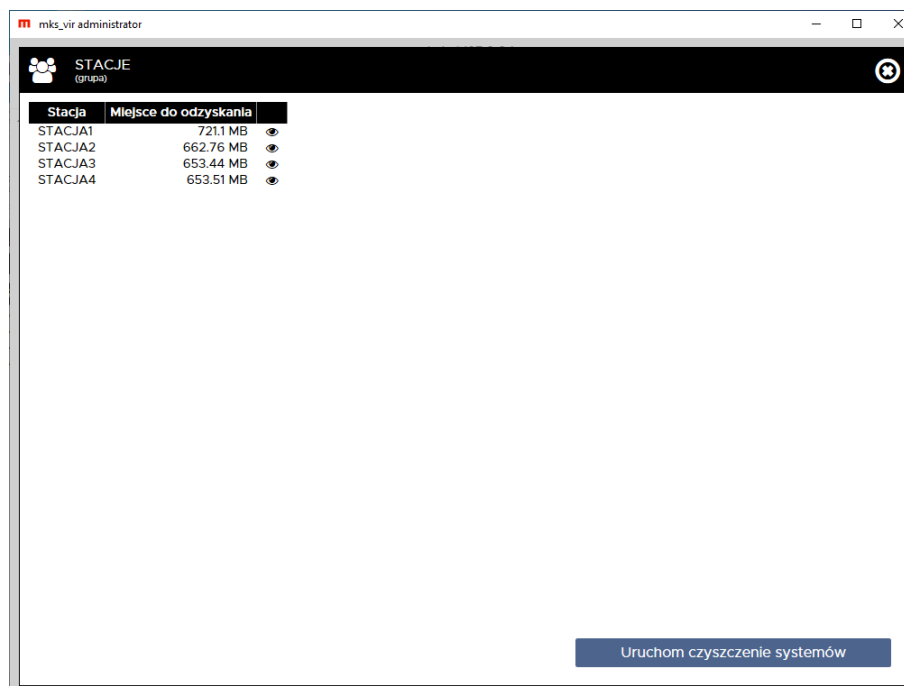
Jeśli jest widoczny napis „**W grupie są stacje z oczekującymi aktualizacjami Windows**”, to znaczy że na części stacji w danej grupie są oczekujące na instalację aktualizacje systemu Windows. Kliknięcie w ten napis powoduje wyświetlenie okna z listą stacji, na których są oczekujące na instalację aktualizacje systemu Windows:



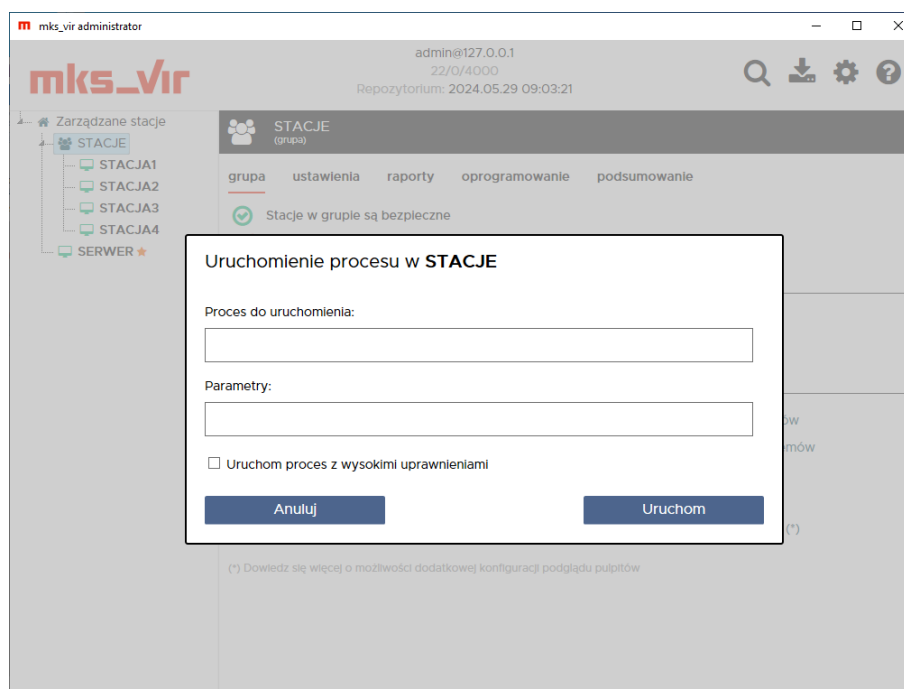
W linii „**Uprawnienia**” podane są informacje, którzy ze zdefiniowanych w ustawieniach konsoli i serwera zarządzającego użytkowników mają prawa dostępu do danej grupy (pozwalające na wyświetlanie i modyfikację parametrów danej grupy); użytkownik **admin** ma zawsze pełne uprawnienia do wszystkich grup i tylko ten użytkownik ma możliwość modyfikacji praw dostępu do grup dla innych zdefiniowanych użytkowników. Wybranie ikony  pozwala na modyfikację praw dostępu do danej grupy.

Przyciski dostępne w tej sekcji pozwalają na:

- **Aktualizacja** – wymuszenie aktualizacji na stacjach w danej grupie
- **Skanowanie szybkie** – wymuszenie wykonania skanowania szybkiego na stacjach w danej grupie
- **Skanowanie pełne** – wymuszenie wykonania skanowania pełnego na stacjach w danej grupie
- **Wyczyść SafeStorage** – usunięcie całej zawartości folderu SafeStorage na stacjach w danej grupie
- **Wyłącz stacje** – wymusza wyłączenie stacji w danej grupie (nie dotyczy stacji z zainstalowanym programem **mks_vir administrator** – stacje oznaczone symbolem ★)
- **Włącz stacje** – wymusza włączenie stacji w danej grupie (oczywiście tylko w przypadku, gdy jest to możliwe za pomocą mechanizmu *Wake On Lan*)
- **Restartuj stacje** – wymusza zrestartowanie stacji w danej grupie
- **Zablokuj stacje** – wymusza zablokowanie stacji w danej grupie
- **Menadżer procesów** – uruchamia podgląd listy procesów stacji w danej grupie, jest możliwe z jego poziomu wymuszenie zamknięcia procesów
- **Czyszczenie systemów** – wyświetla okno z informacjami ile na poszczególnych stacjach można zwolnić miejsca na dyskach oraz pozwala na uruchomienie czyszczenia (czyli usunięcie zbędnych śmieci):



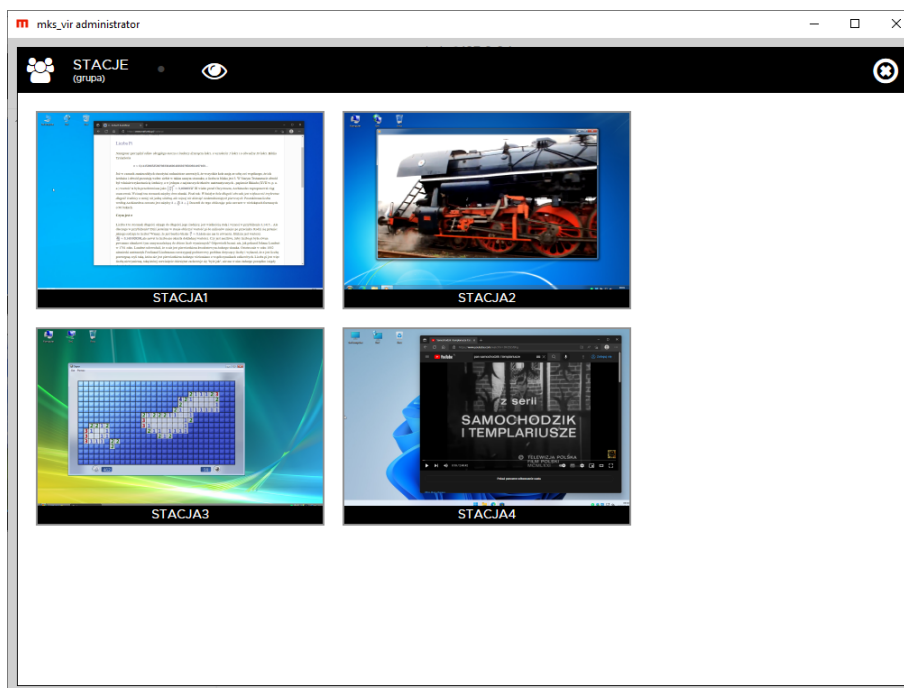
- **Wyślij wiadomość** – umożliwia wysłanie wiadomości do stacji w danej grupie
- **Uruchom proces** – pozwala na wysłanie do stacji w danej grupie polecenia uruchomienia jakiegoś programu:



gdzie:

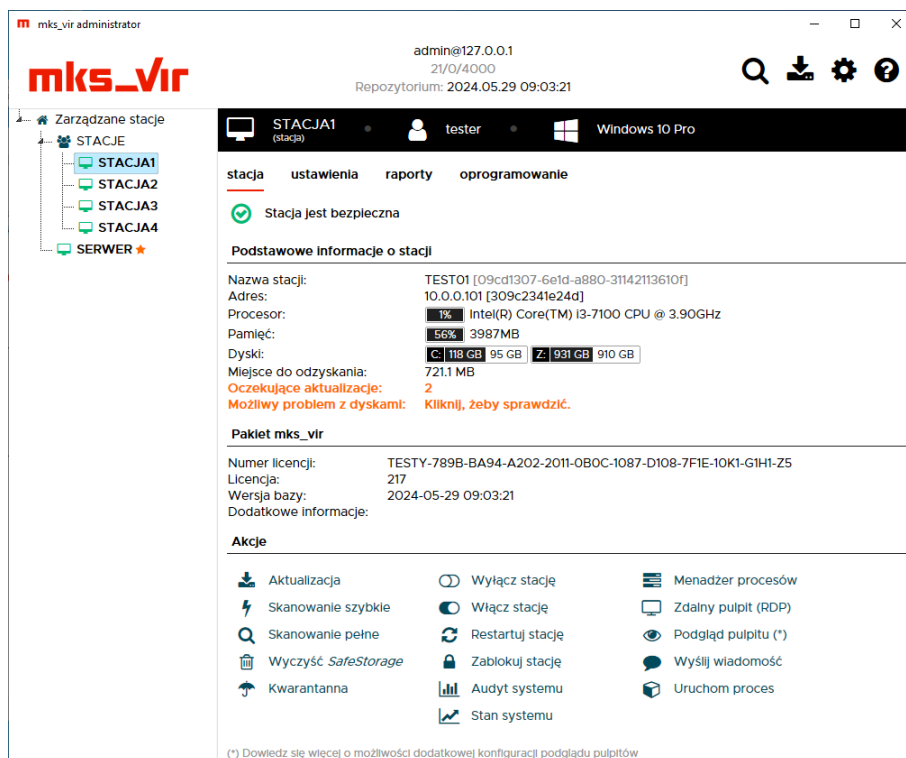
- **Proces do uruchomienia** – tu podajemy nazwę pliku do uruchomienia, jeśli jest to konieczne razem ze ścieżką do tego pliku
- **Parametry** – tu podajemy opcjonalne parametry wywołania procesu
- **Uruchom proces z wysokimi uprawnieniami** – zaznaczenie opcji spowoduje uruchomienie procesu z uprawnieniami systemu, w przeciwnym razie proces będzie uruchomiony z uprawnieniami zalogowanego użytkownika

- **Podgląd pulpitów** – umożliwia wyświetlenie miniatur pulpitów stacji w danej grupie i podglądanie w czasie rzeczywistym działań użytkowników:

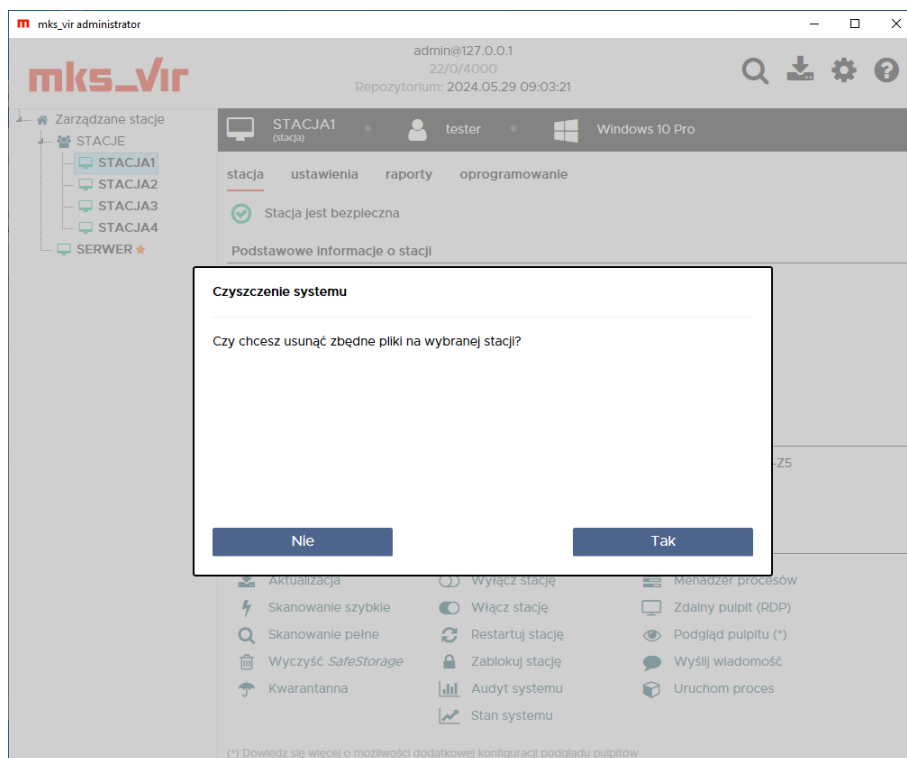


Kliknięcie w miniaturkę powoduje przeniesienie do sekcji danej stacji

Podstawowe informacje o stacji:

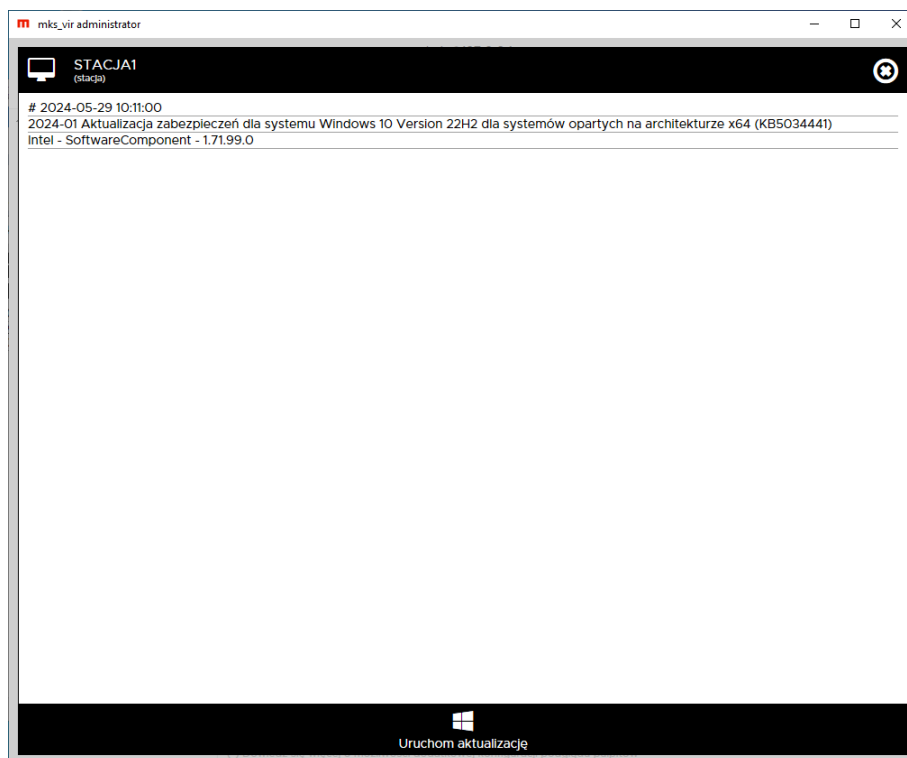


Jeśli jest widoczny napis „**Miejsce do odzyskania**” wraz z wielkością, to znaczy że na tej stacji można zwolnić na dysku tyle miejsca, ile wskazuje wyświetlana wielkość. Kliknięcie umożliwi rozpoczęcie czyszczenia (czyli usunięcie zbędnych śmieci):



Jeśli jest widoczny napis „**Możliwy problem z dyskami: Kliknij, żeby sprawdzić**”, to znaczy że na tej stacji do systemu są zgłaszane jakieś problemy dyskowe. Kliknięcie w ten napis umożliwi obejrzenie szczegółów.

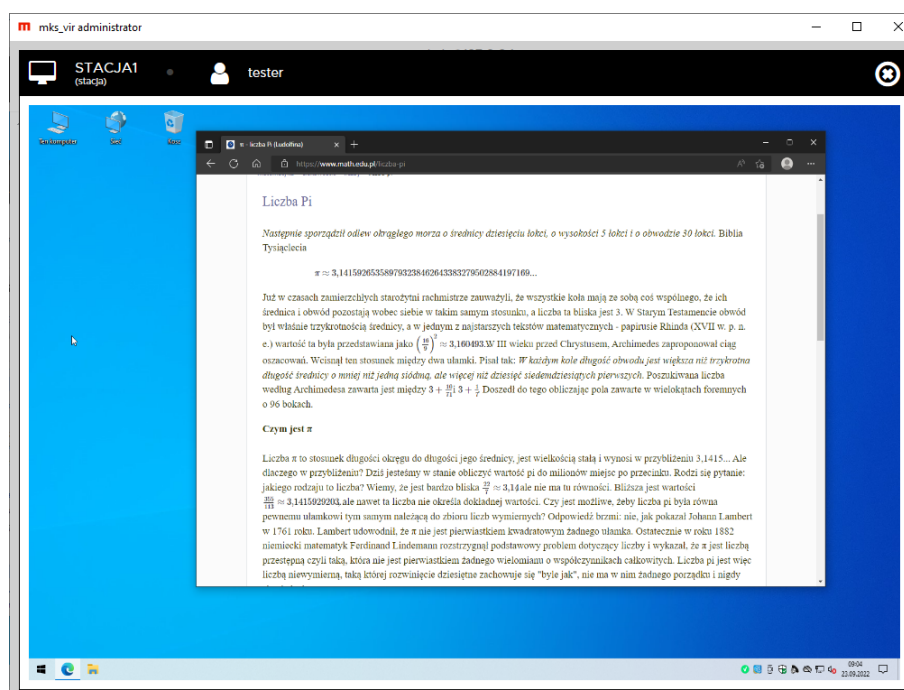
Jeśli jest widoczny napis „**Oczekujące aktualizacje**”, to znaczy że na tej stacji są oczekujące na instalację aktualizacje systemu Windows. Kliknięcie w ten napis powoduje wyświetlenie okna z listą oczekujących aktualizacji systemu Windows:



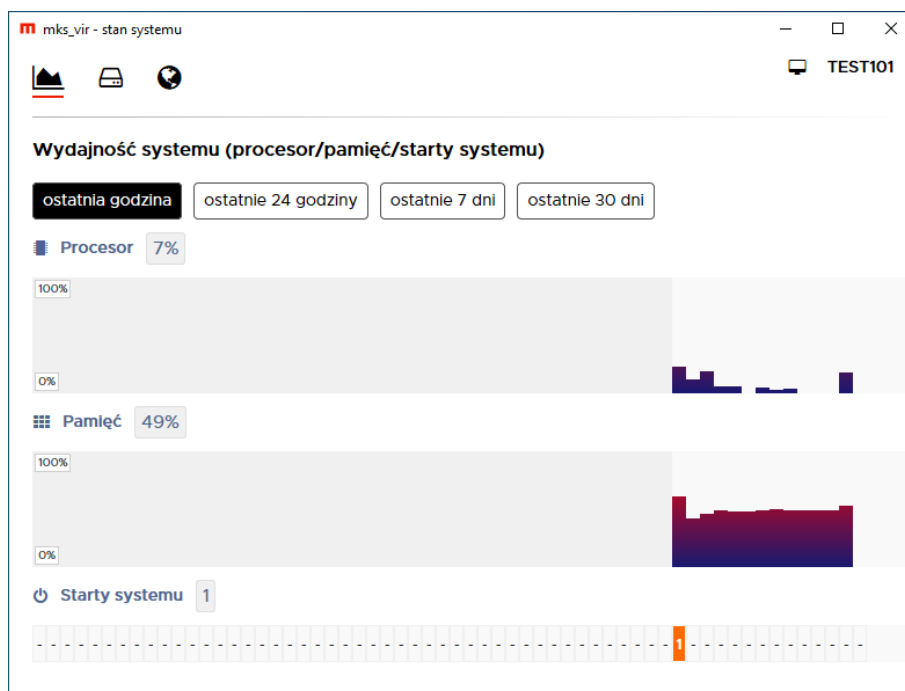
Wybranie „**Uruchom aktualizacje**” powoduje wymuszenie instalacji oczekujących aktualizacji systemu Windows na danej stacji.

Przyciski dostępne w tej sekcji pozwalają na:

- **Aktualizacja** – wymuszenie aktualizacji na danej stacji
- **Skanowanie szybkie** – wymuszenie wykonania skanowania szybkiego na danej stacji
- **Skanowanie pełne** – wymuszenie wykonania skanowania pełnego na danej stacji
- **Wyczyść SafeStorage** – usunięcie całej zawartości folderu SafeStorage na danej stacji
- **Kwarantanna** – zarządzanie zawartością kwarantanny na danej stacji
- **Wyłącz stację** – wymusza wyłączenie danej stacji (nie dotyczy stacji z zainstalowanym programem **mks_vir administrator** – stacje oznaczone symbolem ★)
- **Włącz stację** – wymusza włączenie danej stacji (oczywiście tylko w przypadku, gdy jest to możliwe za pomocą mechanizmu *Wake On Lan*)
- **Restartuj stację** – wymusza zrestartowanie danej stacji
- **Zablokuj stację** – wymusza zablokowanie danej stacji
- **Audyt systemu** – umożliwia wygenerowanie i wysłanie audytu systemu z danej stacji w celu jego dalszej analizy w dziale analiz **mks_vir**
- **Menadżer procesów** – uruchamia podgląd listy procesów danej stacji, jest możliwe z jego poziomu wymuszenie zamknięcia procesów
- **Zdalny pulpit** – uruchomienie zdalnego połączenia ze stacją za pomocą RDP (tylko w przypadku, gdy system operacyjny na stacji pozwala na takie połączenia oraz możliwość taka została wcześniej na stacji włączona)
- **Podgląd pulpitu** – umożliwia podglądanie w czasie rzeczywistym działań użytkownika na danej stacji:



- **Wyślij wiadomość** – umożliwia wysłanie wiadomości do danej stacji
- **Stan systemu** – moduł pozwalający na ocenę wybranych parametrów pracy systemu:
 - Wydajność systemu:

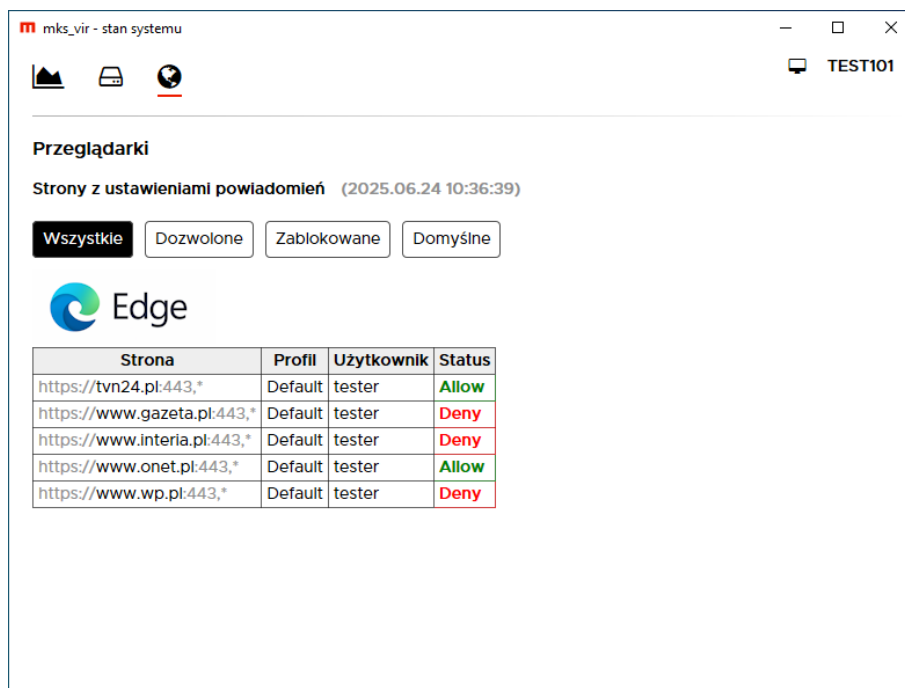


- Dyski:

Model	Serial	Rozmiar	Partycje
ST1000DM010-2EP102	Z9AP4S4Z	931.5 GB	Z:
ADATA SU800	2H4320092706	119.2 GB	C:

Status dysków fizycznych (S.M.A.R.T.)					
ADATA SU800 C:					
Status	Parameter	Current	Worst	Threshold	Data
✓	Raw read error rate (1)	100	100	0	0
⚠	Reallocated sector count (5)	100	100	0	1
✓	Power-on hours count (9)	100	100	0	3837
✓	Power cycle count (12)	100	100	0	1795
✓	Power-off retract count (192)	100	100	0	48
✓	HDD temperature (194)	100	100	0	40
✓	Reallocation count (196)	100	100	16	2

- Przeglądarki:



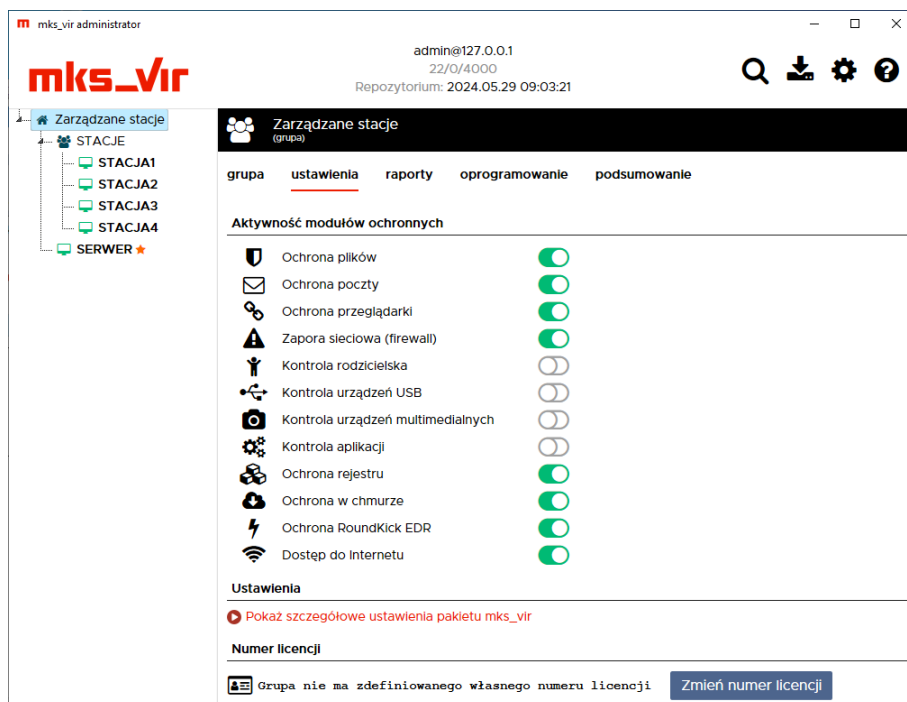
- **Uruchom proces** – pozwala na wysłanie do stacji polecenia uruchomienia jakiegoś programu


Ustawienia:

Konfiguracja wybranego elementu. Każdy element (grupa lub stacja) może posiadać konfigurację indywidualną lub korzystać z konfiguracji grupy nadrzędnej

W przypadku, gdy dla danego elementu (grupy lub stacji) jest ustawiona konfiguracja indywidualna, to jest możliwość szybkiej zmiany aktywności modułów ochronnych; w przeciwnym wypadku jest to tylko podgląd stanu (aktywny lub nieaktywny) tych modułów

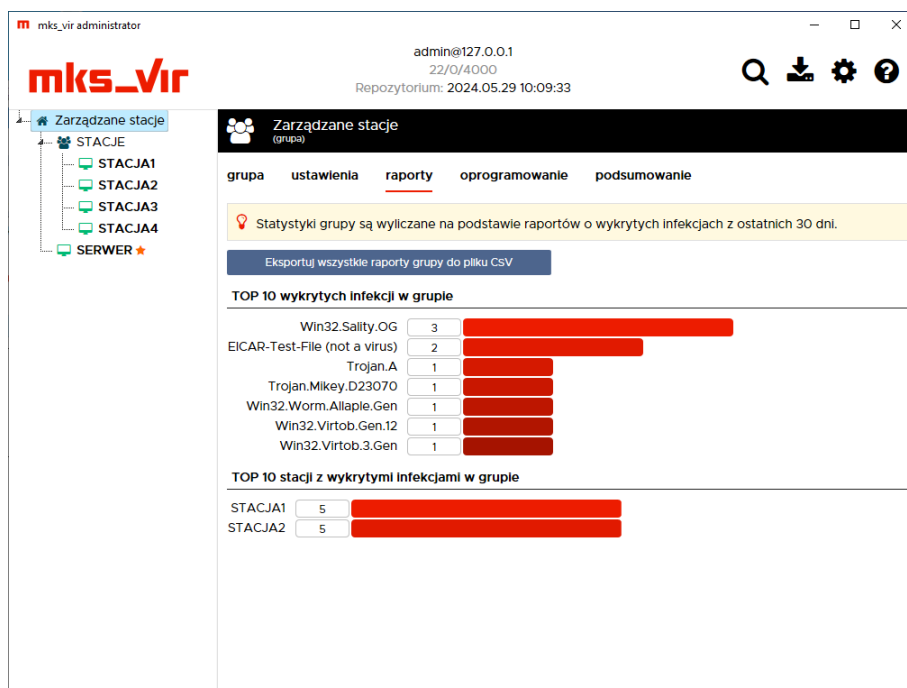
Jeżeli w danym elemencie (grupie lub stacji) nie ma zdefiniowanego numeru licencji, to stacje pracują na podstawie numeru licencji podanego przy ich instalacji



Elementem nie mającym odpowiednika w konfiguracji jest **Dostęp do Internetu**, który służy do włączania (zielony) lub wyłączania (czerwony) dostępu do sieci Internet na zarządzanych stacjach, przy czym jego działanie jest uzależnione od aktywności **Zapory sieciowej (firewall)** – jeśli zapora będzie nieaktywna, to zmiana stanu **Dostępu do Internetu** nie będzie powodowała żadnych efektów. Aktywna blokada dostępu do sieci Internet na stacjach jest sygnalizowana zmienionym wyglądem ikony programu **mks_vir** na 

Raporty:

W przypadku grup w raportach widoczne są zbiorcze statystyki o ew. wykrytych na stacjach infekcjach:



Możliwe jest też zapisanie wszystkich raportów grupy do pliku tekstowego w formacie CSV (potem można taki plik przetwarzać np. w Microsoft Excel, LibreOffice Calc itp.) za pomocą przycisku „Eksportuj wszystkie raporty grupy do pliku CSV”

W przypadku stacji jest to tabela z widocznymi w niej poszczególnymi raportami z aktywności programu:

The screenshot shows the mks_vir administrator interface. The left sidebar displays a tree view of managed stations: STACJE (STACJA1, STACJA2, STACJA3, STACJA4) and SERWER. The main content area is for STACJA1 (stacja) and shows the 'raporty' tab. The interface includes a search bar, a user profile (tester), and system information (Windows 10 Pro). Below the navigation tabs, there are filters for 'Raporty z dnia: 2025-03-17', 'Pokaż historię przeglądanych stron', and 'Pokaż aktywność sieciową'. The main table displays the following data:

Data	Zdarzenie	Status
2025-03-17 10:11:57	Aktualizacja pakietu	✓
2025-03-17 10:10:08	Aktualizacja pakietu	✓
2025-03-17 10:07:31	Aktualizacja pakietu	✓
2025-03-17 07:42:05	Aktualizacja pakietu	✓
2025-03-17 04:41:49	Aktualizacja pakietu	✓
2025-03-17 01:41:19	Aktualizacja pakietu	✓

At the bottom right, there is a link: 'Pokaż tylko raporty o infekcjach'.

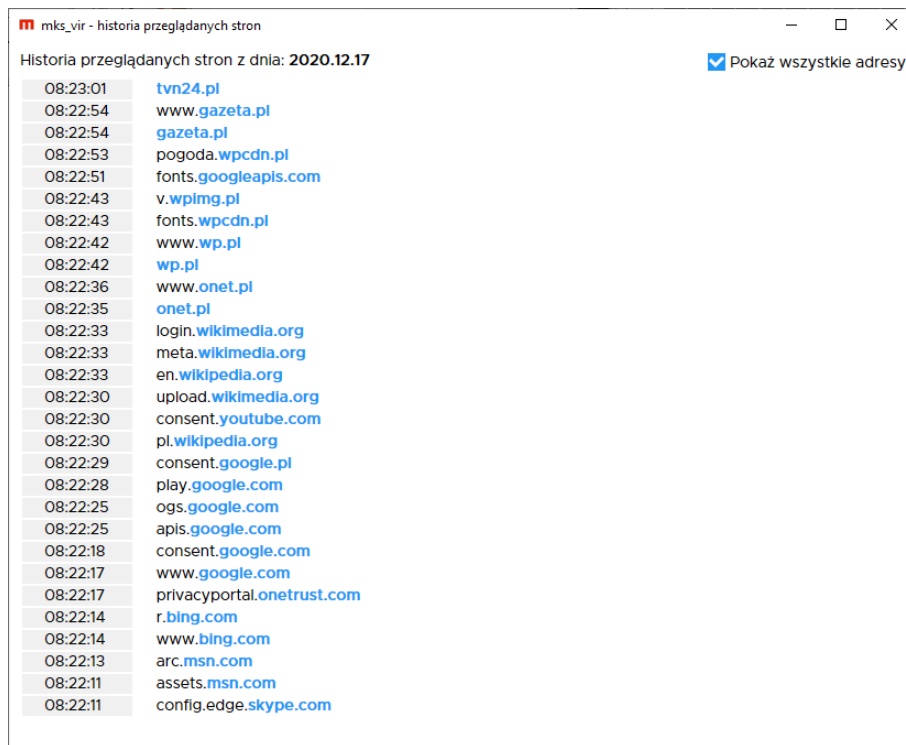
Po wybraniu „Pokaż tylko raporty o infekcjach” pojawią się tylko raporty z wykrytymi infekcjami w ostatnich 30 dniach; powrót do normalnego wyświetlania raportów jest możliwy przez wybranie „Wróć do domyślnego widoku raportów”:

The screenshot shows the mks_vir administrator interface with the 'raporty' tab selected. The main content area displays 'Raporty o infekcjach z ostatnich 30 dni'. The table shows the following data:

Data	Zdarzenie	Status
2025-03-13 12:38:45	Skanowanie folderów i plików	Infekcja
2025-03-13 12:38:08	Skanowanie folderów i plików	Infekcja
2025-03-13 12:33:32	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:33:20	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:33:09	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:32:59	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:32:47	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:30:35	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 12:30:16	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:22	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:22	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-13 11:52:18	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:25:06	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:57	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:47	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:39	Monitor wykrył szkodliwy obiekt	Infekcja
2025-03-11 08:24:25	Monitor wykrył szkodliwy obiekt	Infekcja

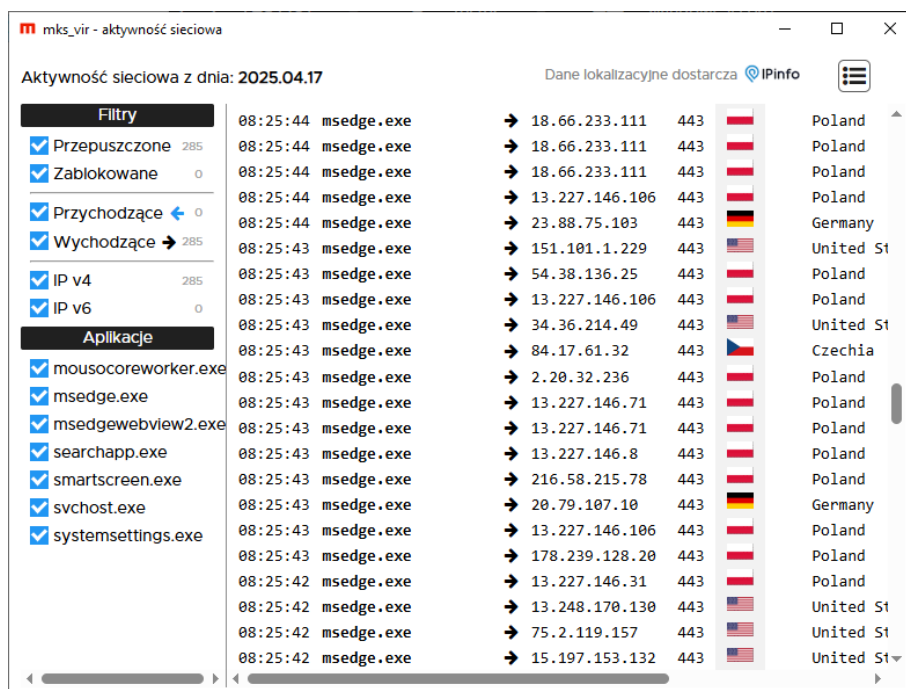
At the bottom right, there is a link: 'Wróć do domyślnego widoku raportów'.

Po wybraniu „Pokaż historię przeglądanych stron” pojawi się okno pozwalające na przeglądanie aktywności internetowej użytkowników danej stacji:



Kliknięcie w dowolną domenę spowoduje skopiowanie jej do systemowego schowka, co w rezultacie pozwala na łatwe tworzenie własnych reguł w konfiguracji (grupy lub stacji)

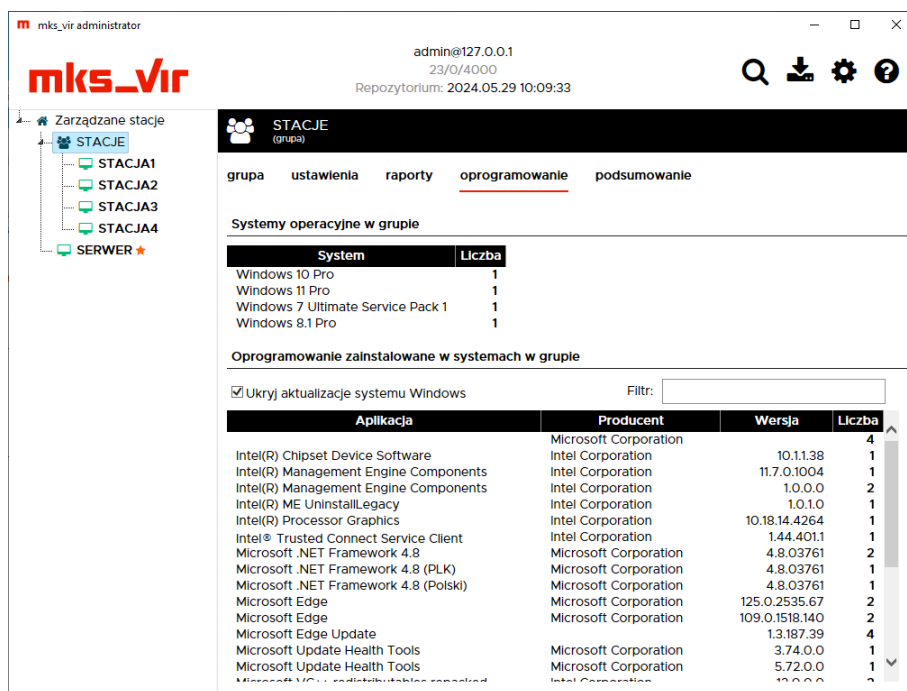
Po wybraniu „Pokaż aktywność sieciową” pojawi się okno pozwalające na przeglądanie aktywności sieciowej systemu i zainstalowanych aplikacji:



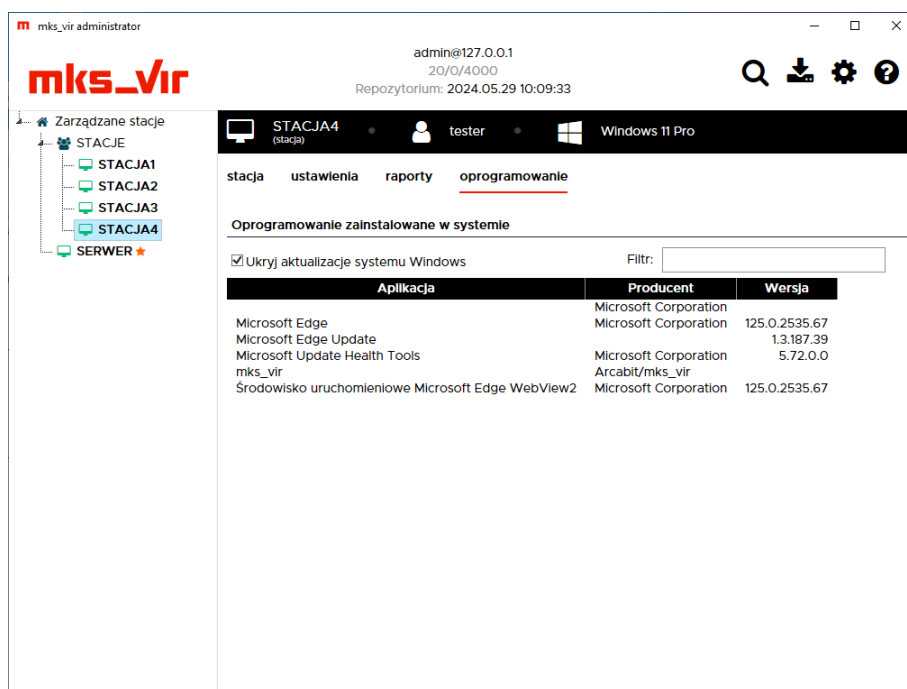
- **Filtry** – pozwala na filtrację aktywności:
 - dla połączeń przepuszczonych lub **zablokowanych**
 - dla połączeń przychodzących (←) lub wychodzących (→)
 - dla połączeń na protokołach **IP v4** lub **IP v6**
- **Aplikacje** – pozwala na filtrację aktywności połączeń dla określonych aplikacji

Oprogramowanie:

W przypadku grupy jest widoczna statystyka typów i ilości systemów na stacjach oraz zbiorcza lista zainstalowanych na stacjach aplikacji:



W przypadku stacji jest widoczna lista zainstalowanych na niej aplikacji:



Podsumowanie:

Tabela ze zbiorczą informacją na temat stacji z danej grupy (nazwa, system, sprzęt, wersja bazy mks_vir, czas ważności licencji mks_vir itp.):

The screenshot shows the 'mks_vir administrator' interface. At the top, it displays the user 'admin@127.0.0.1' and the repository '22/0/4000' with a timestamp of '2024.05.29 10:09:33'. The main content area is titled 'STACJE (grupa)' and has tabs for 'grupa', 'ustawienia', 'raporty', 'oprogramowanie', and 'podsumowanie'. A button 'Eksportuj podsumowanie grupy do pliku CSV' is visible. Below the table, there is a checkbox for 'Widok podstawowy'.

Nazwa	IP	System	Procesor	Pamięć	Użytkownicy	Wersja bazy	Abonament	Oczekujące aktualizacje	% Pamięć	Pr
STACJA1	10.0.0.101	Windows 10 Pro 6.2 X64	Intel(R) Core (TM) i3-7100 CPU @ 3.90GHz	3987	tester	2024-05-29 09:03:21	217	2	55%	19
STACJA2	10.0.0.102	Windows 7 Ultimate 6.1 X64 SP 1.0	Intel(R) Core (TM) i3-4130 CPU @ 3.40GHz	3983	tester	2024-05-29 09:03:21	217	0	28%	0'
STACJA3	10.0.0.103	Windows 8.1 Pro 6.2 X86	Intel(R) Core (TM) i3 CPU 540 @ 3.07GHz	3447	tester	2024-05-29 09:03:21	217	1	26%	0'
STACJA4	10.0.0.104	Windows 11 Pro 6.2 X64	Intel(R) Core (TM) i3-9100 CPU @ 3.60GHz	16246	tester	2024-05-29 09:03:21	217	2	16%	0'

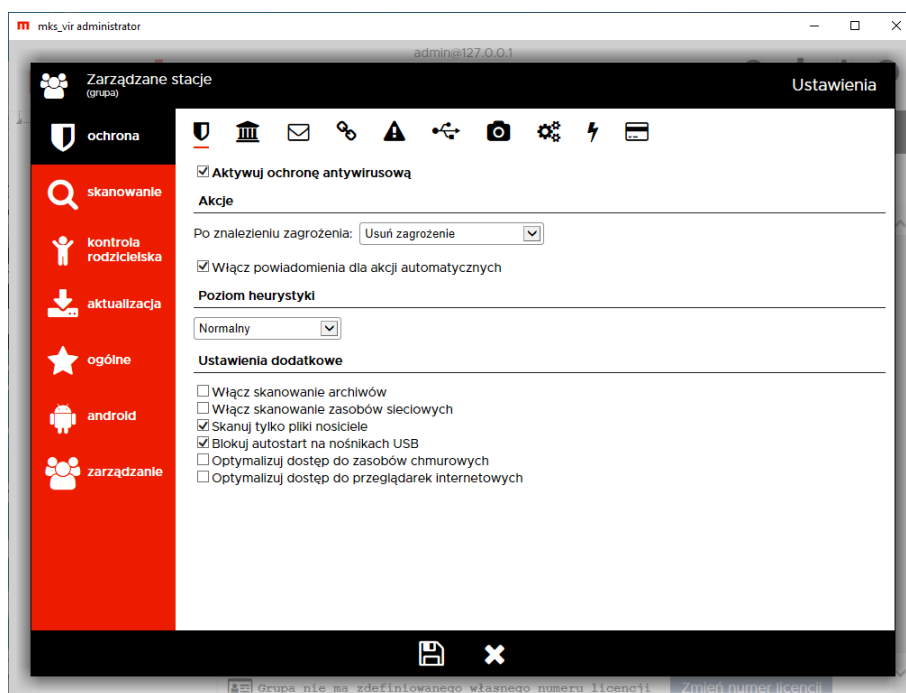
Możliwe jest też zapisanie podsumowania grupy do pliku tekstowego w formacie CSV (po-tem można taki plik przetwarzać np. w Microsoft Excel, LibreOffice Calc itp.) za pomocą przy-cisku „Eksportuj podsumowanie grupy do pliku CSV”

mks_vir administrator automatycznie tworzy, aktualizuje i udostępnia po protokole HTTP repozytorium aktualizacyjne dla podłączonych stacji **mks_vir**, które z takiego repozytorium mogą się aktualizować, nie jest więc konieczna żadna oddzielna konfiguracja

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

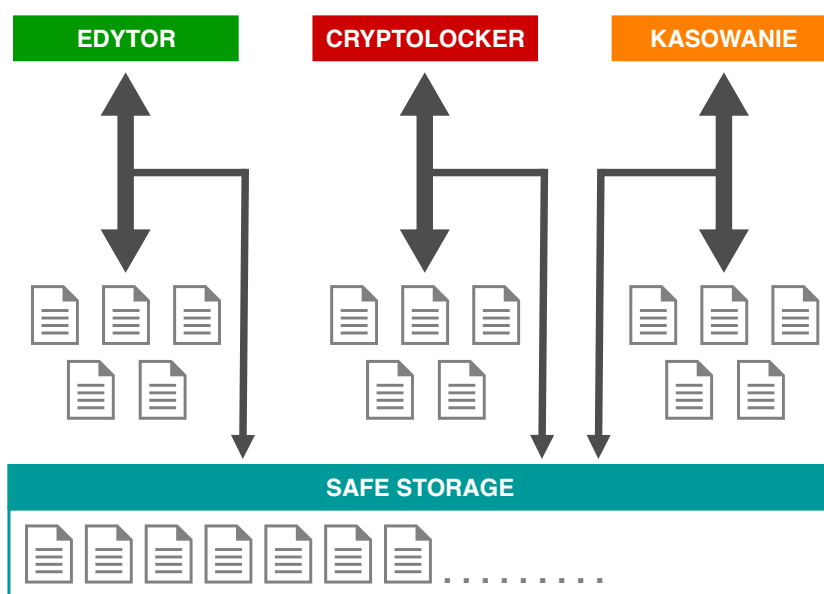
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

Ustawienia dodatkowe:

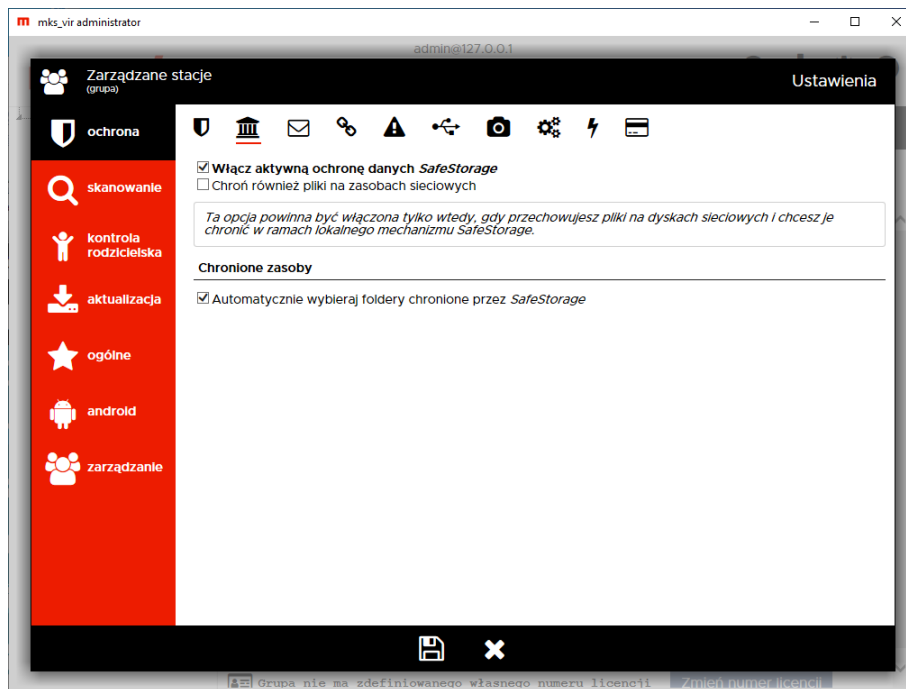
- **Włącz skanowanie archiwów** – włącza możliwość skanowania zawartości plików typu ZIP, RAR, 7Z itp.
- **Włącz skanowanie zasobów sieciowych** – włącza sprawdzanie podłączonych zasobów sieciowych; należy mieć na uwadze, że aktywność tej opcji może spowolnić dostęp do plików znajdujących się na podłączonych zasobach sieciowych
- **Skanuj tylko nośniki** – opcja powoduje, że sprawdzane są tylko pliki będące domyślnymi nośnikami zagrożeń, jak np. pliki EXE, COM, JS, VBS itp.
- **Blokuj autostart na nośnikach USB** – uniemożliwia automatyczne uruchomienie z podłączonych 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.



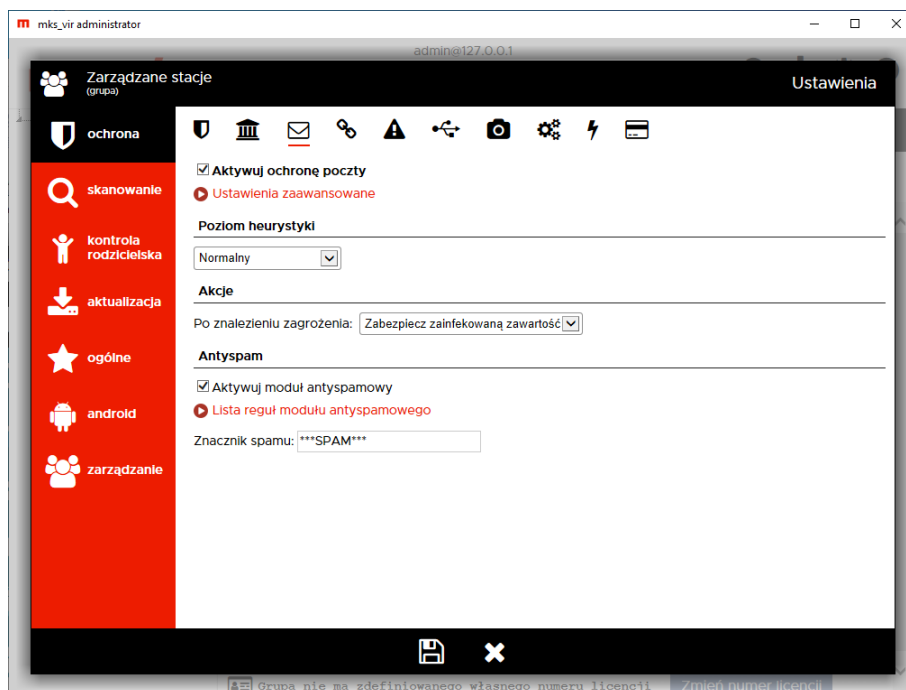
Włącz aktywną ochronę danych *SafeStorage* – włącza mechanizm ochrony danych, szczególnie przed zagrożeniami szyfrującymi (np. Cryptolocker)

- **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

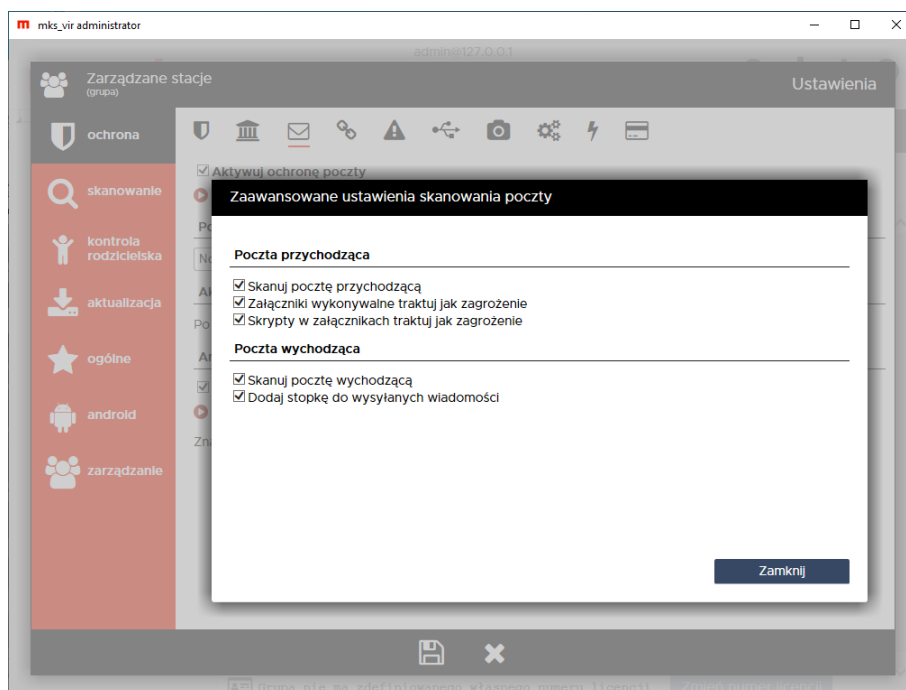
- **Automatycznie wybieraj foldery chronione przez *SafeStorage*** – przy włączonej opcji program domyślnie chroni dane na wszystkich dyskach lokalnych dostępnych w komputerze; jej wyłączenie umożliwia wybranie, które foldery mają być chronione

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:



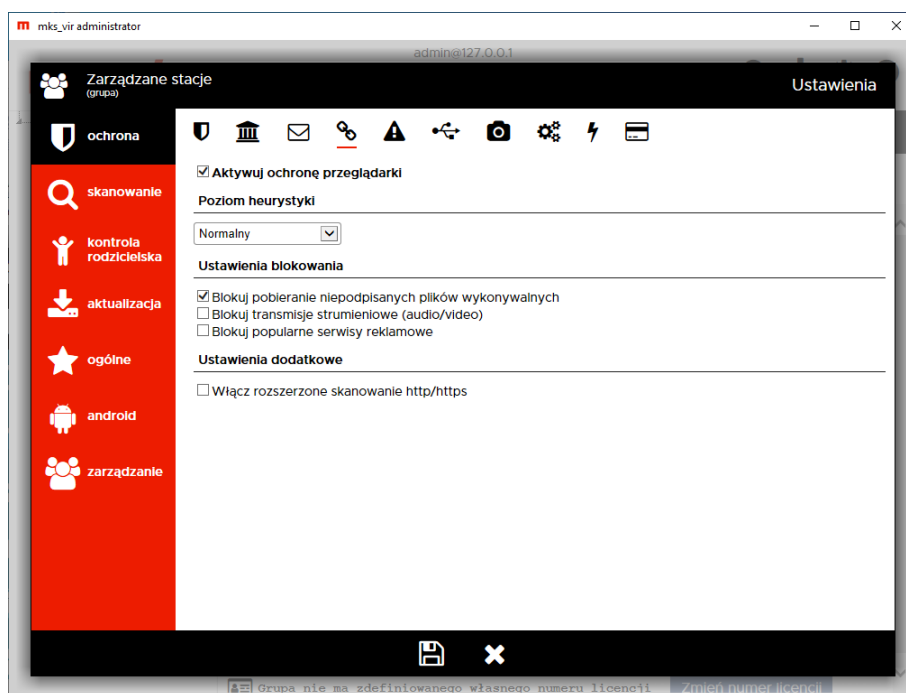
Poziom heurystyki – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. „fałszywych alarmów”

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 - oryginalny 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”

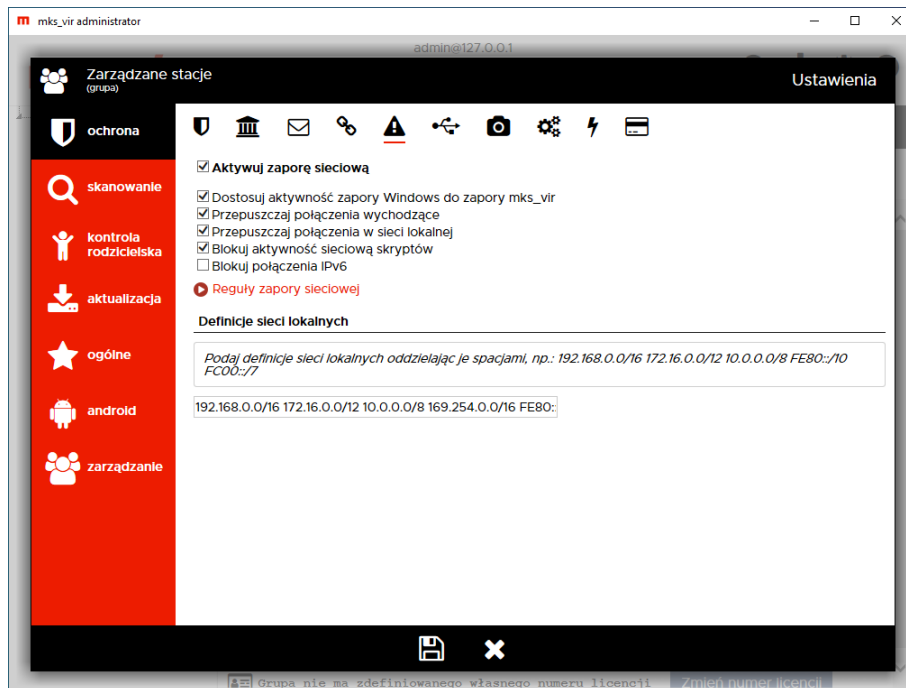
Ustawienia blokowania

- **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 blokadę wszelkiego rodzaju transmisji strumieniowych (co na przykład uniemożliwia słuchanie stacji radiowych przez internet)
- **Blokuj popularne serwisy reklamowe** – włączenie tej opcji powoduje blokadę 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

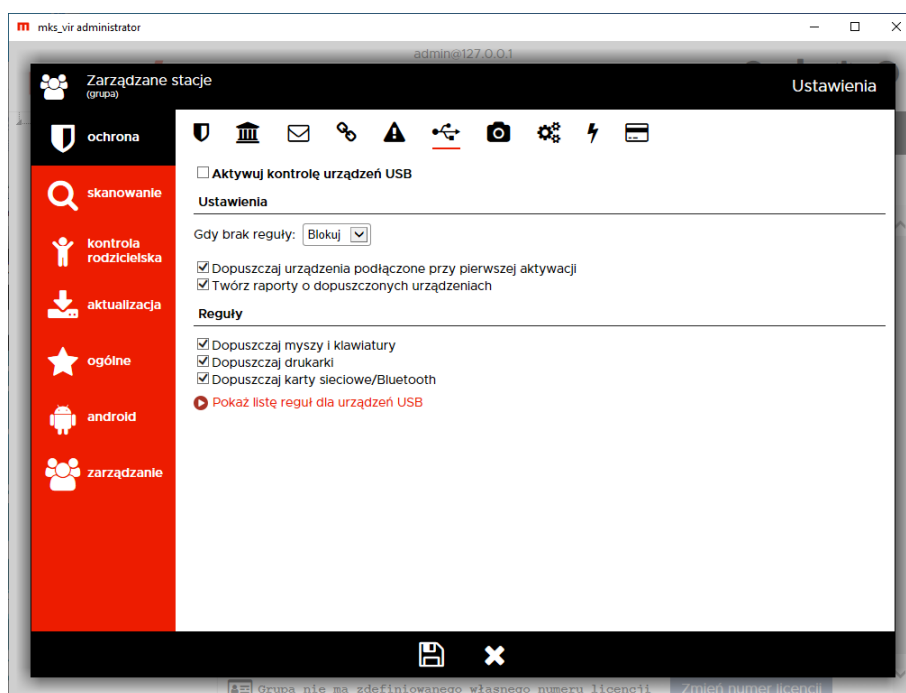
- **Dostosuj aktywność zapory Windows do zapory mks_vir** – aktywność tej opcji umożliwia automatyczne przełączanie aktywności zapory Windows w zależności od aktywności zapory mks_vir; aktywacja zapory mks_vir wyłącza zaporę Windows, zaś dezaktywacja zapory mks_vir włącza zaporę Windows, dzięki czemu w systemie stale jest aktywna zaporę
- **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.)
- **Blokuj połączenia IPv6** – opcja ta blokuje wszelkie połączenia realizowane przy pomocy protokołu IPv6

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_podsiéci

Ochrona → Kontrola urządzeń USB:



Aktywuj kontrolę urządzeń USB – aktywuje moduł kontroli urządzeń USB

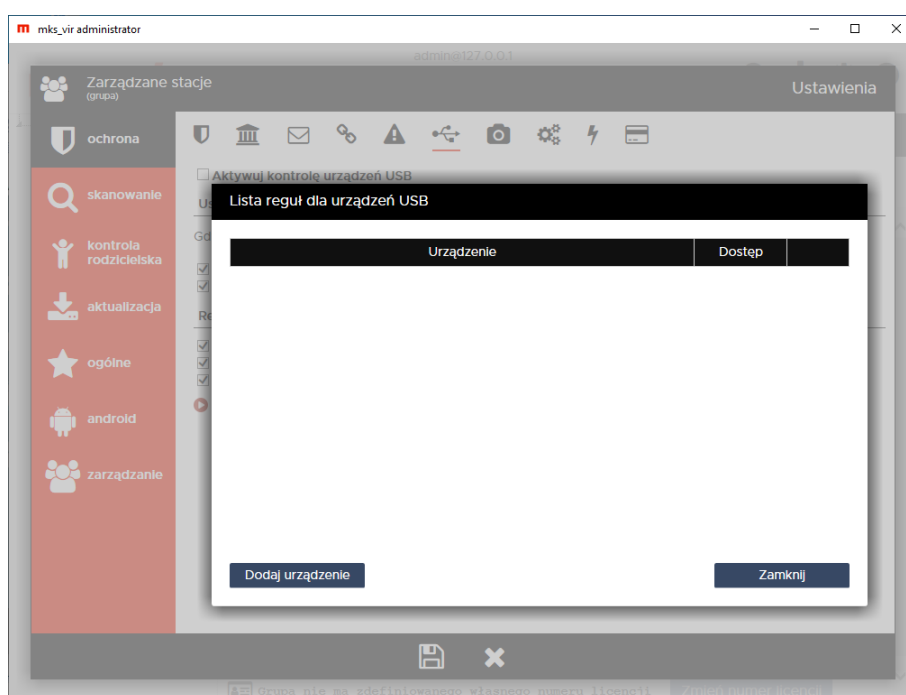
Ustawienia – umożliwia konfigurację modułu kontroli urządzeń USB

- **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
 - **Dopuszczaj** – 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 „Dopuszczaj” (przy podłączaniu nowych urządzeń USB)

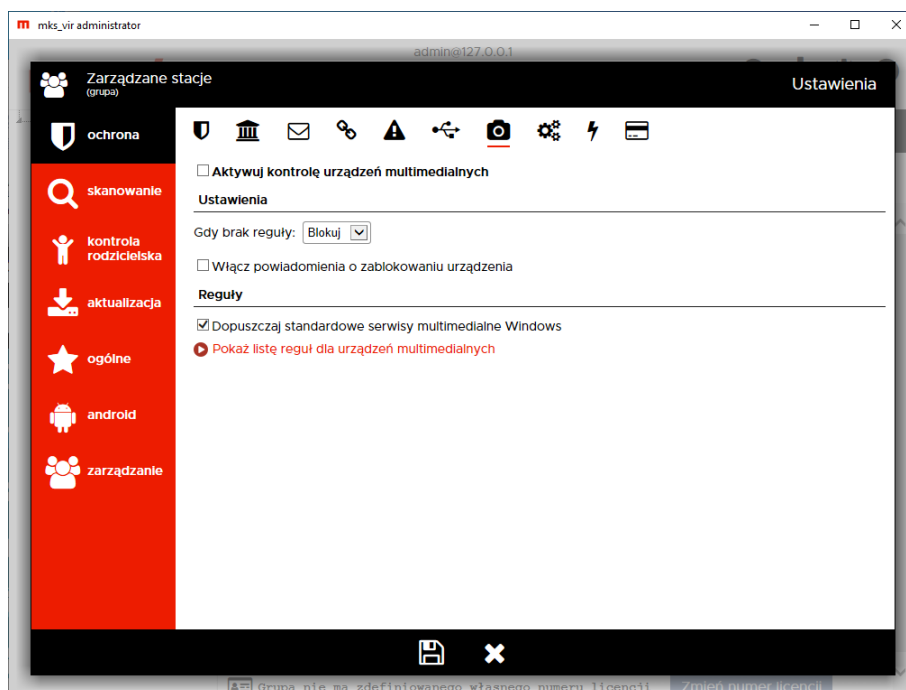
Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających podłączane urządzenia USB

- **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

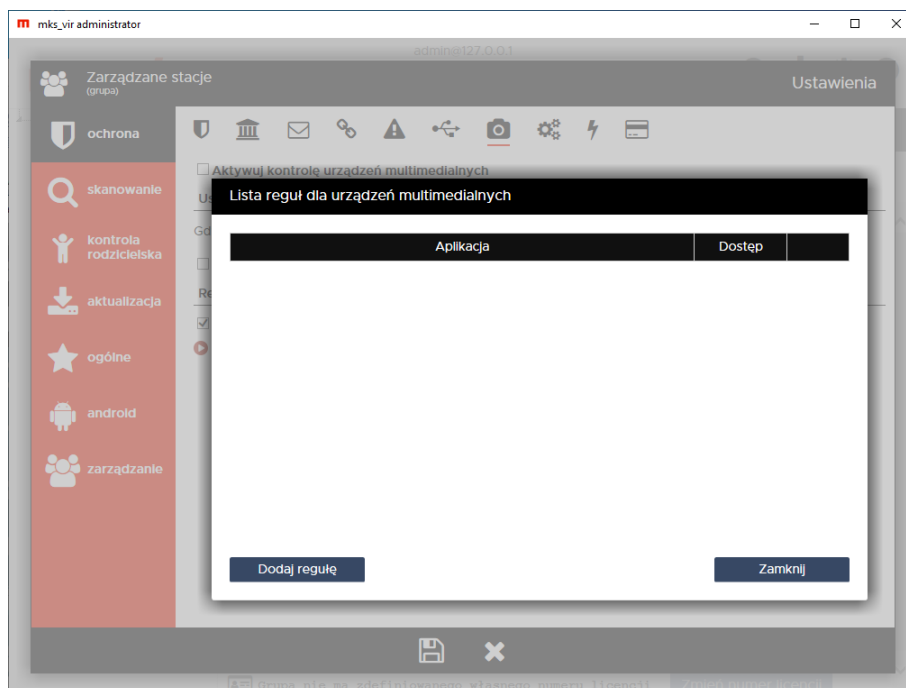
Ustawienia – umożliwia konfigurację modułu kontroli urządzeń multimedialnych

- **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
 - **Dopuszcz** – 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”

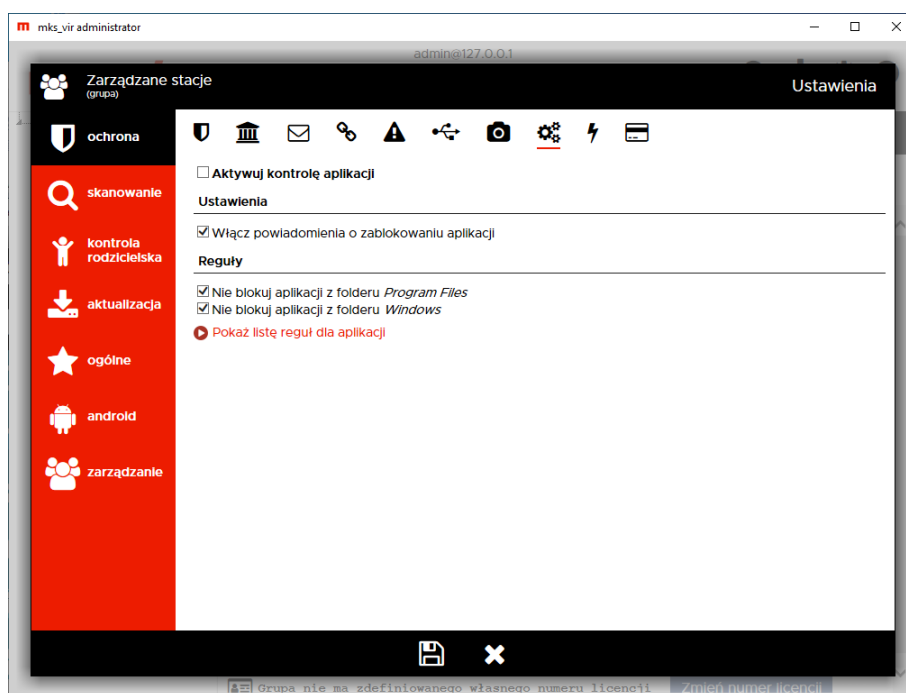
Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających dostęp do urządzeń multimedialnych przez aplikacje

- **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

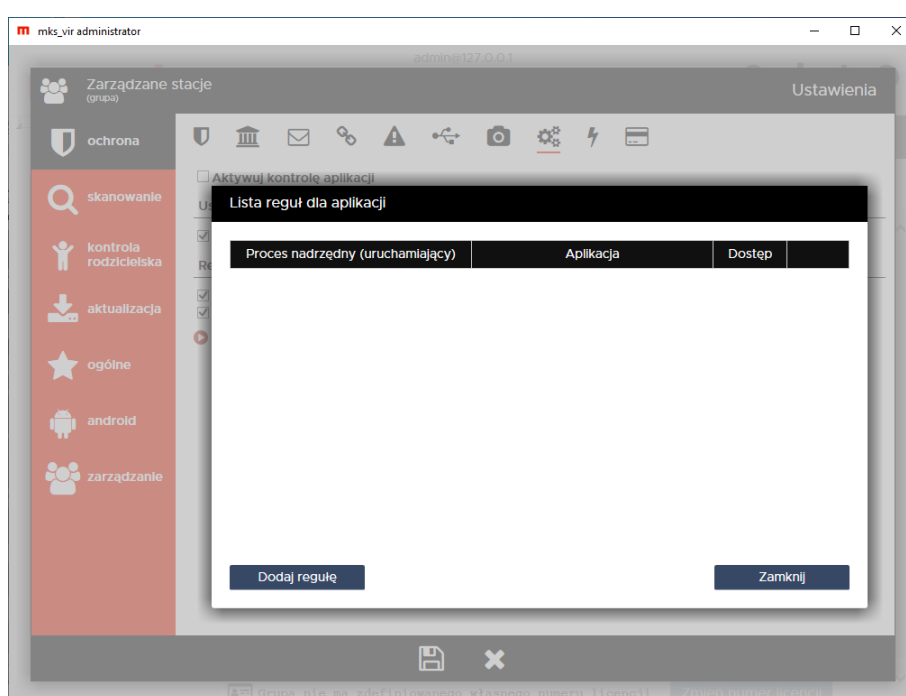
- **Włącz powiadomienia o zablokowaniu aplikacji** – włącza wyświetlanie okien powiadomień modułu kontroli aplikacji w przypadku zablokowania próby uruchomienia aplikacji, dla której została zdefiniowana reguła blokująca

Reguły – umożliwia definiowanie lub modyfikację reguł blokujących lub dopuszczających 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!

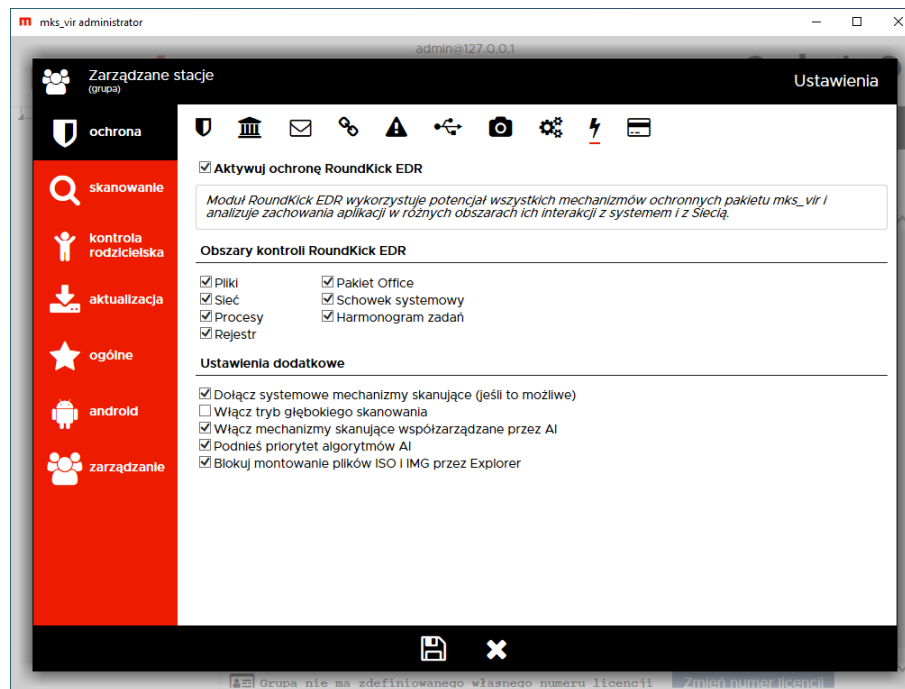
Pokaż listę reguł dla aplikacji – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających uruchamianie aplikacji:



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*

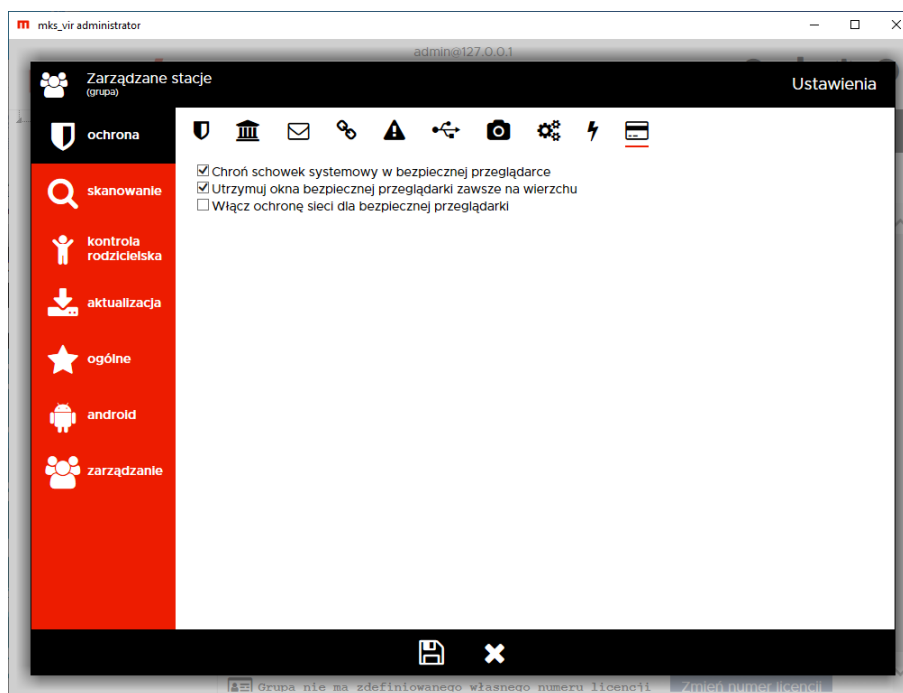
Obszary kontroli RoundKick EDR – pozwala na określenie w jakich zakresach mają być aktywne zaawansowane mechanizmy ochronne *RoundKick EDR*

- **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
- **Harmonogram zadań** – monitoruje zmiany w systemowym harmonogramie zadań, przeprowadzając szczegółową analizę zachowań potencjalnie złośliwych procesów w sposób zintegrowany z usługami chmury obliczeniowej **mks_vir**, wykorzystując mechanizmy uczenia maszynowego i heurystyczne modele detekcji zagrożeń

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

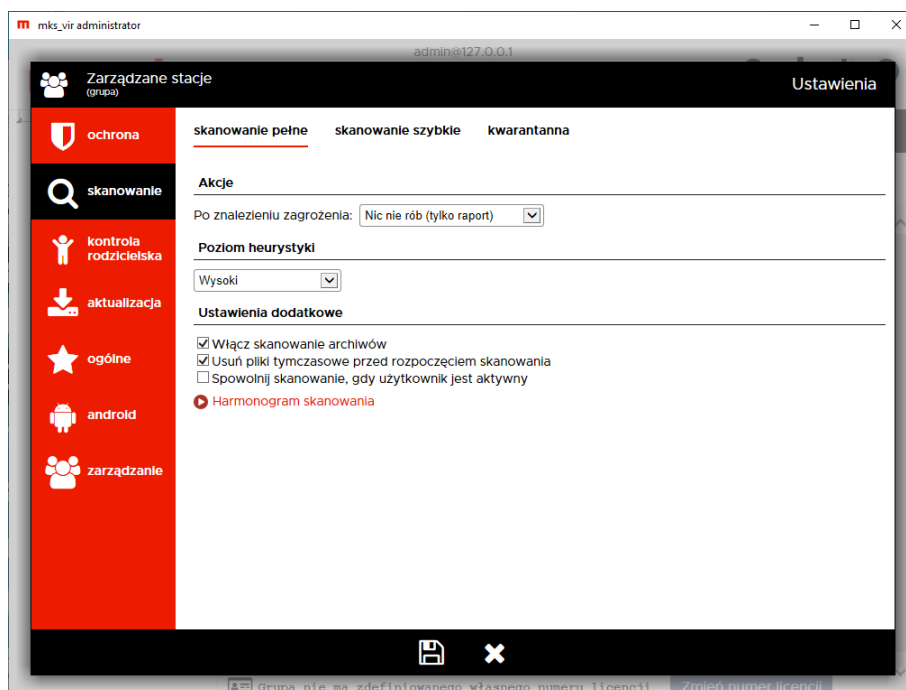
- **Dołącz systemowe mechanizmy skanujące (jeśli to możliwe)** – wyszukuje i wykorzystuje różne moduły skanujące, o ile jakieś są dostępne w systemie
- **Włącz tryb głębokiego skanowania** – włącza zaawansowane mechanizmy skanowania i emulacji celem dokładniejszej analizy skanowanych obiektów
uwaga! włączenie opcji może powodować zauważalne wydłużenie czasów skanowania
- **Włącz mechanizmy skanujące współzarządzane przez AI** – dołączenie do puli mechanizmów skanujących algorytmów i baz zagrożeń zaimplementowanych ze znaczącym udziałem sztucznej inteligencji operującej na dużych zbiorach danych o najnowszych zagrożeniach i wektorach ataków
- **Podnieś priorytet algorytmów AI** – podwyższa priorytet mechanizmów współzarządzanych przez AI w strukturze silników skanujących
- **Blokuj montowanie plików ISO i IMG przez Explorer** – blokuje możliwość montowania obrazów dyskowych typu ISO lub IMG w systemie przez *Eksploratora plików* (wiele rodzajów zagrożeń jest przenoszonych w postaci tego typu plików)

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 wykonywana po zakończeniu pełnego skanowania komputera, do wyboru są następujące możliwości:

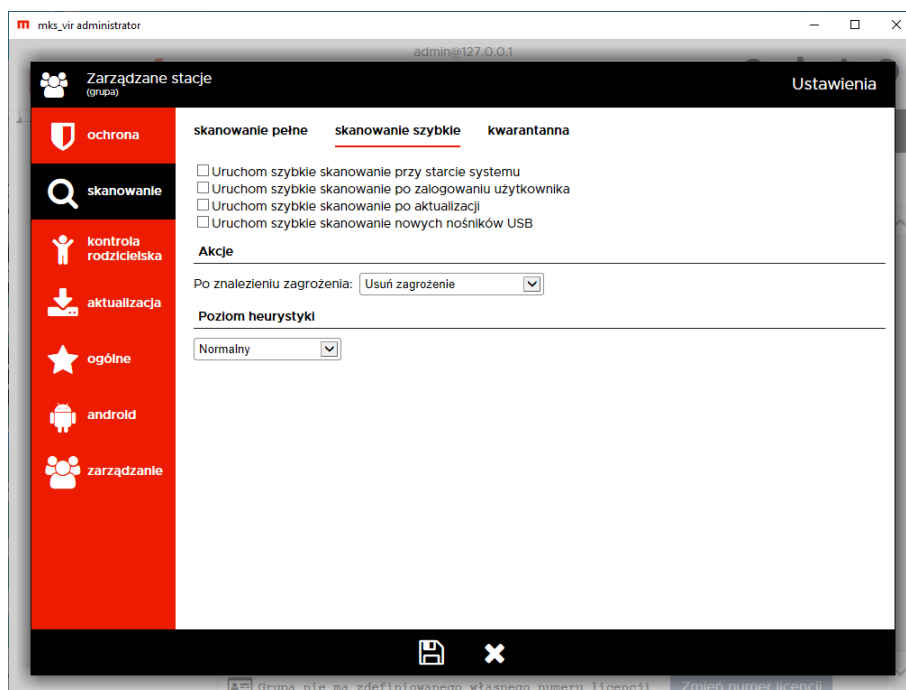
- **Usuń zagrożenia** – leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- **Skasuj plik** – kasuje zainfekowane pliki
- **Przenieś do kwarantanny** – przenosi zainfekowane pliki do folderu kwarantanny **mks_vir**
- **Nic nie rób (tylko raport)** – ew. znalezione 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:

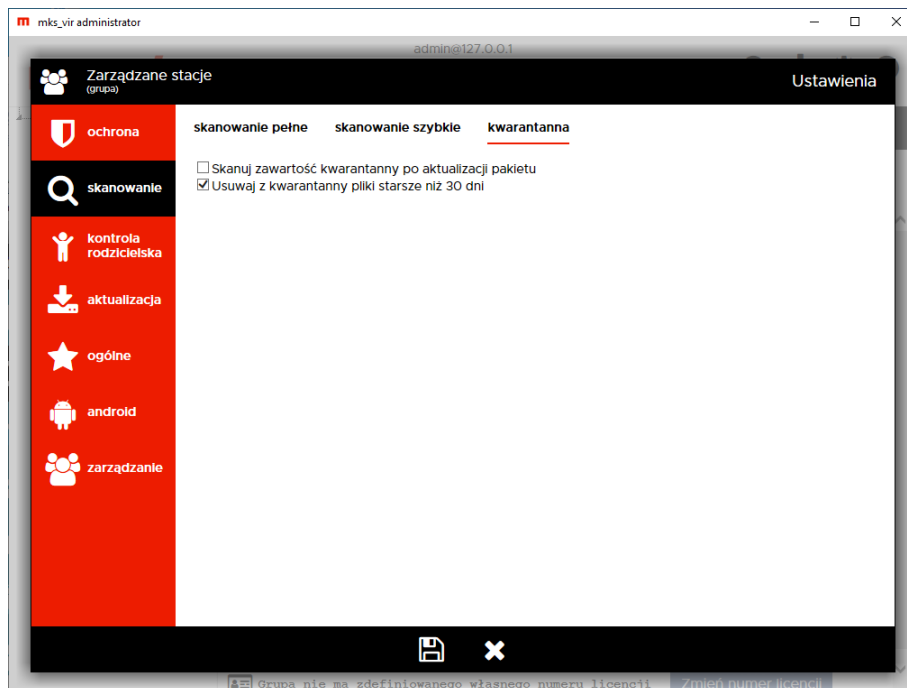
- przy starcie systemu
- po zalogowaniu użytkownika
- po aktualizacji programu mks_vir
- po podłączeniu nośnika USB – skanowana jest wtedy zawartość takiego nośnika

Akcje – umożliwia wybranie akcji, która będzie wykonywana 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”

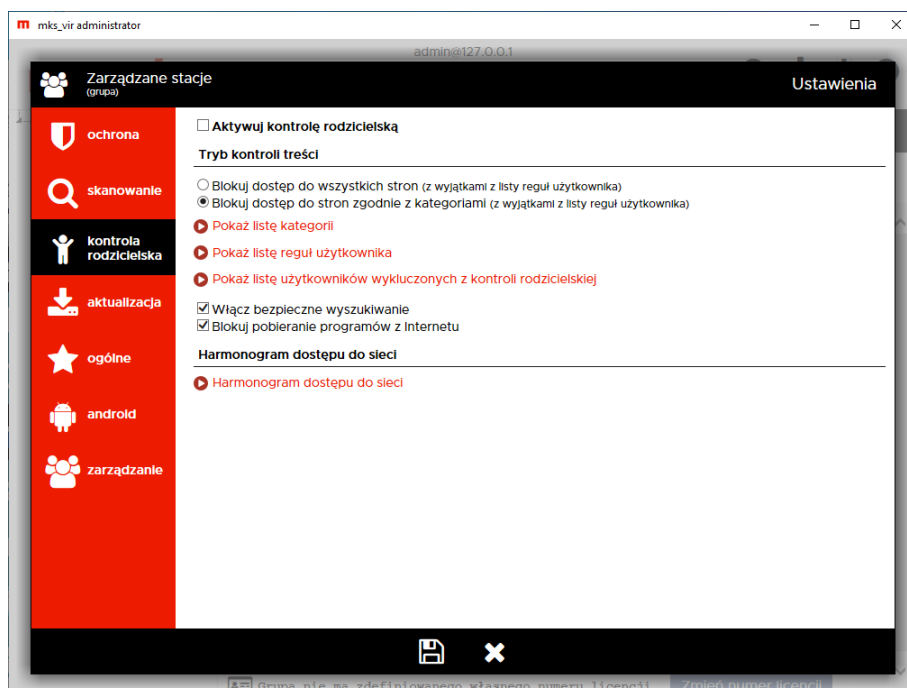
Skanowanie → Kwarantanna:



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 jakiegokolwiek pliki
- **Usuwać 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

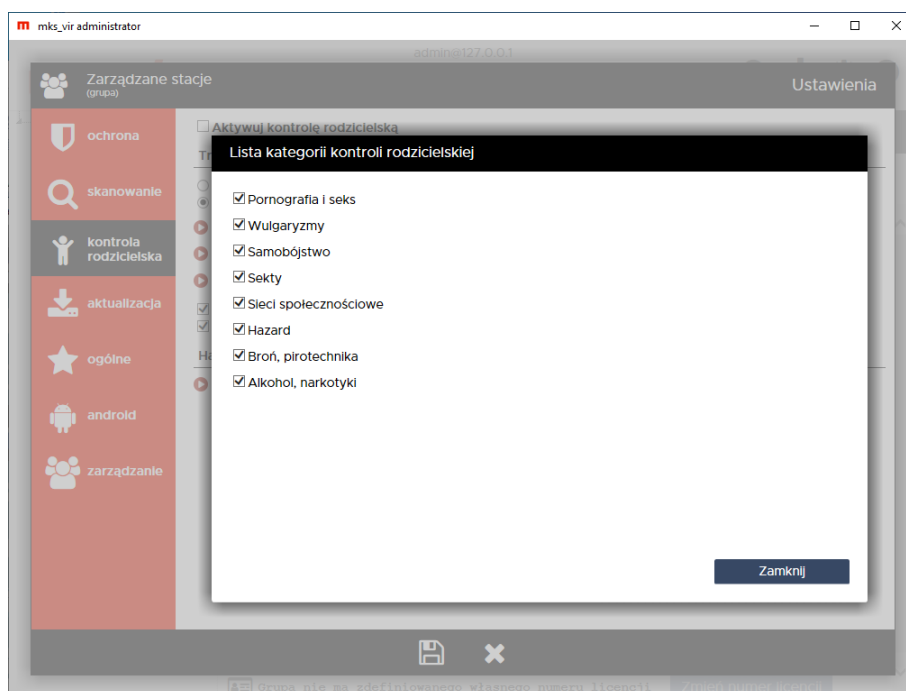
Kontrola rodzicielska:



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”:



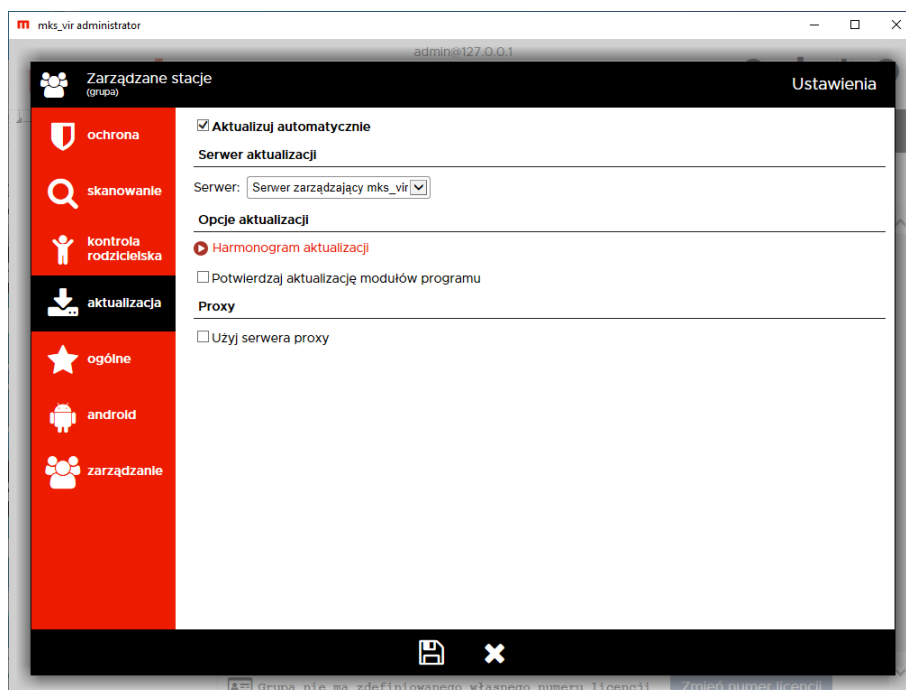
Pokaż listę reguł użytkownika – umożliwia zdefiniowanie własnych reguł przepuszczających lub blokujących w oparciu o adresy lub frazy (słowa kluczowe)

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

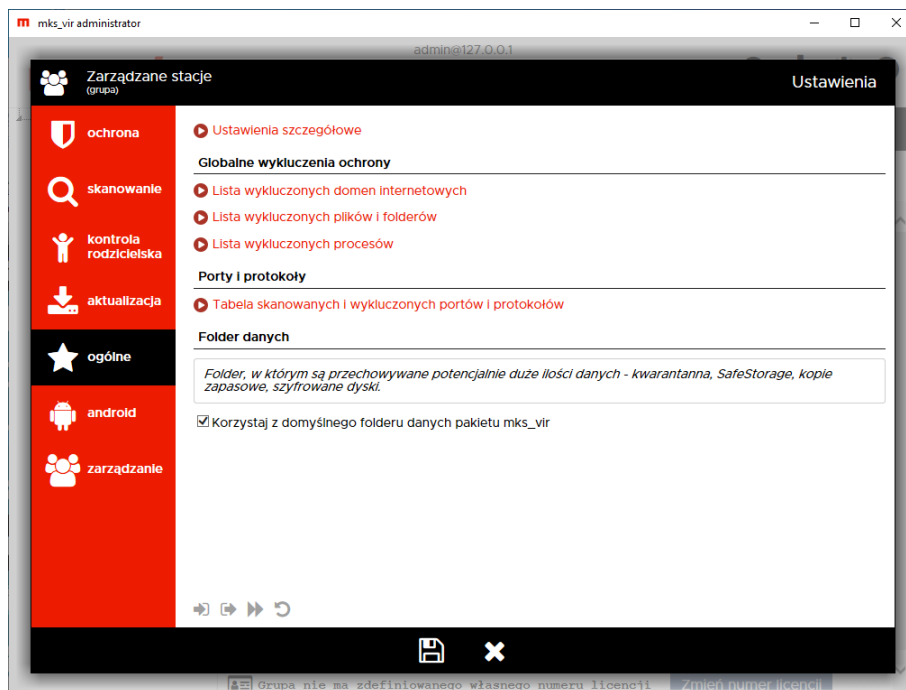
Opcje aktualizacji:

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

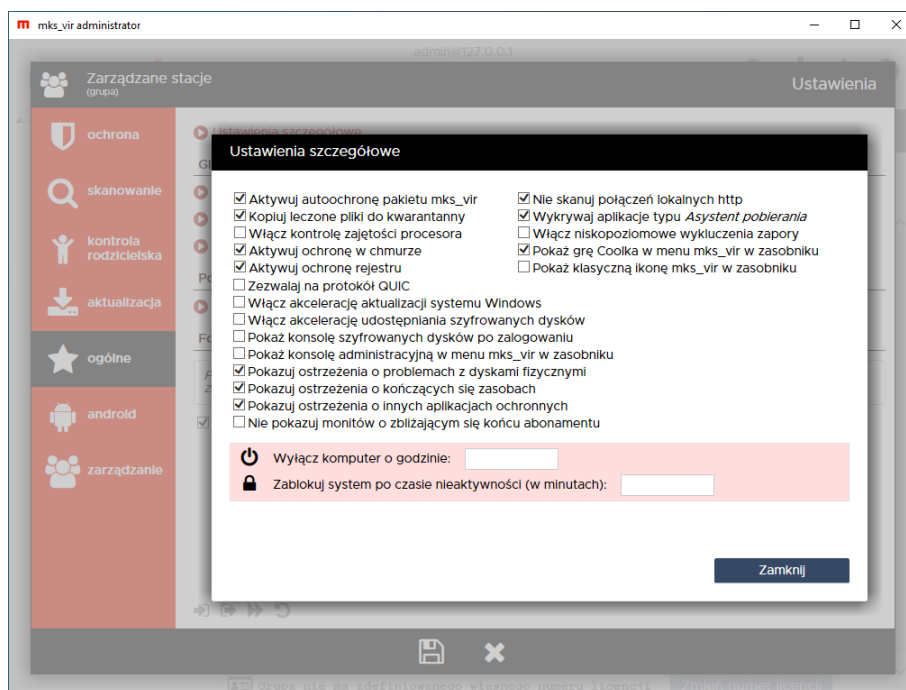
- **Potwierdź aktualizację modułów programu** – włączenie tej opcji powoduje, że na stacjach w przypadku konieczności aktualizacji modułów programowych (a więc innych niż bazy antywirusowe i silniki skanujące) pojawi się pytanie, czy tego dokonać; w niektórych przypadkach samoczynna aktualizacja takich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

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

Ogólne:



Ustawienia szczegółowe – umożliwiają dostosowanie 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**
- **Kopij leczone pliki do kwarantanny** – tworzy w kwarantannie programu **mks_vir** kopie plików leczonych lub kasowanych; funkcja pomocna w przypadku, gdyby była konieczność przywrócenia oryginalnych 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
- **Pokazuj ostrzeżenia o innych aplikacjach ochronnych** – włącza powiadomienia informujące o zainstalowanych i aktywnych w systemie innych aplikacjach ochronnych (antywirusowych), co może być potencjalnym źródłem spadku wydajności, konfliktów z różnymi programami, a nawet destabilizacji pracy systemu
- **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

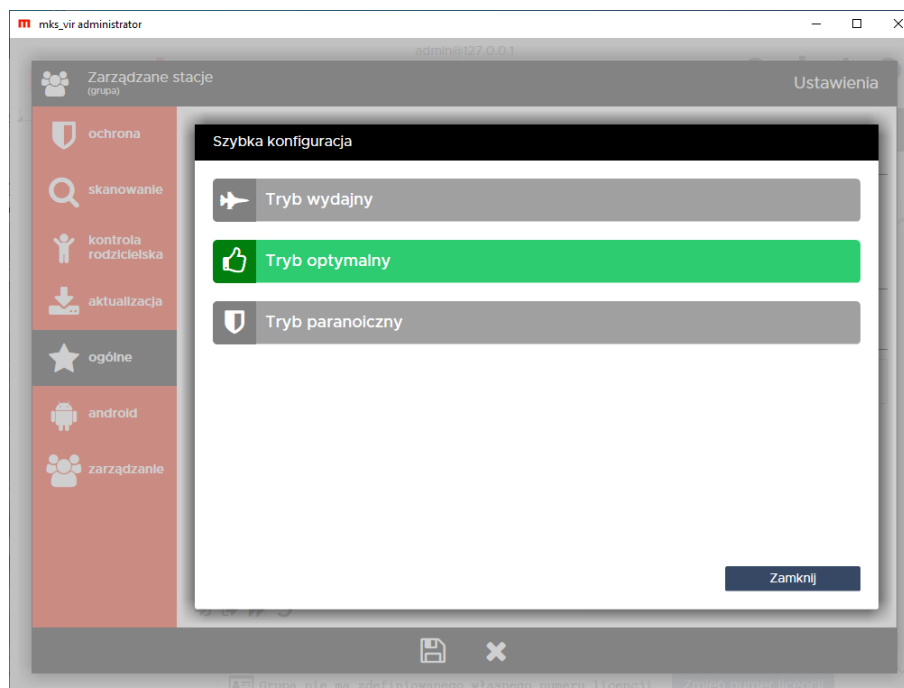
Globalne wykluczenia ochrony – umożliwia zdefiniowanie obiektów, dla których nie będzie działała żadna ochrona, korzystanie z tych ustawień wymaga dużej rozwagi:

- **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**

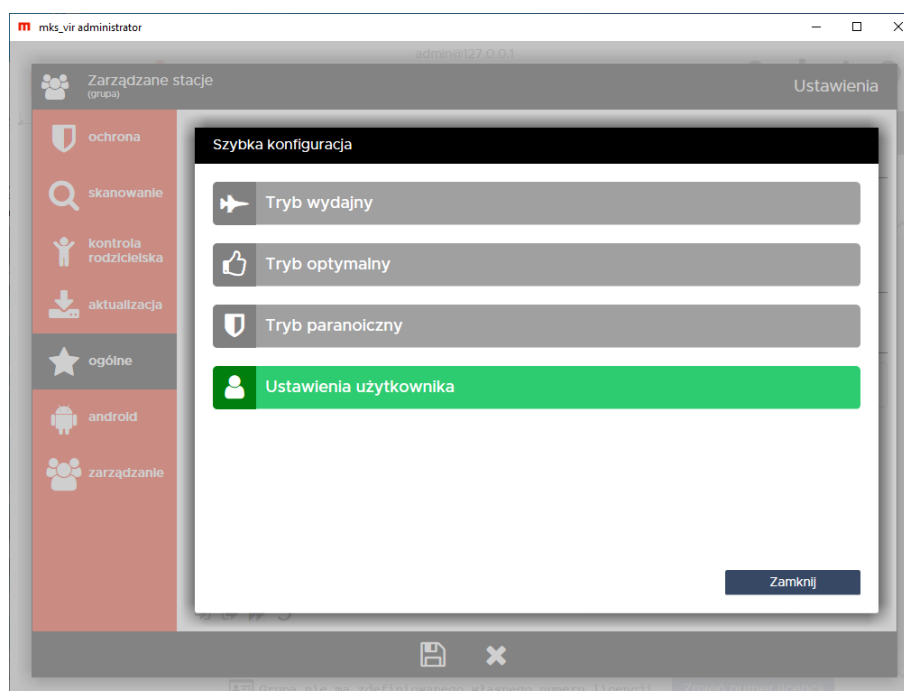
Porty i protokoły – umożliwia zdefiniowane dla których portów mają działać moduły ochrony poczty, ochrony przeglądarki i kontroli rodzicielskiej oraz jakie porty mają być w ogóle wyłączone spod kontroli, również w zaporze programu **mks_vir**; definiuje się je w **Tabeli skanowanych i wykluczonych portów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

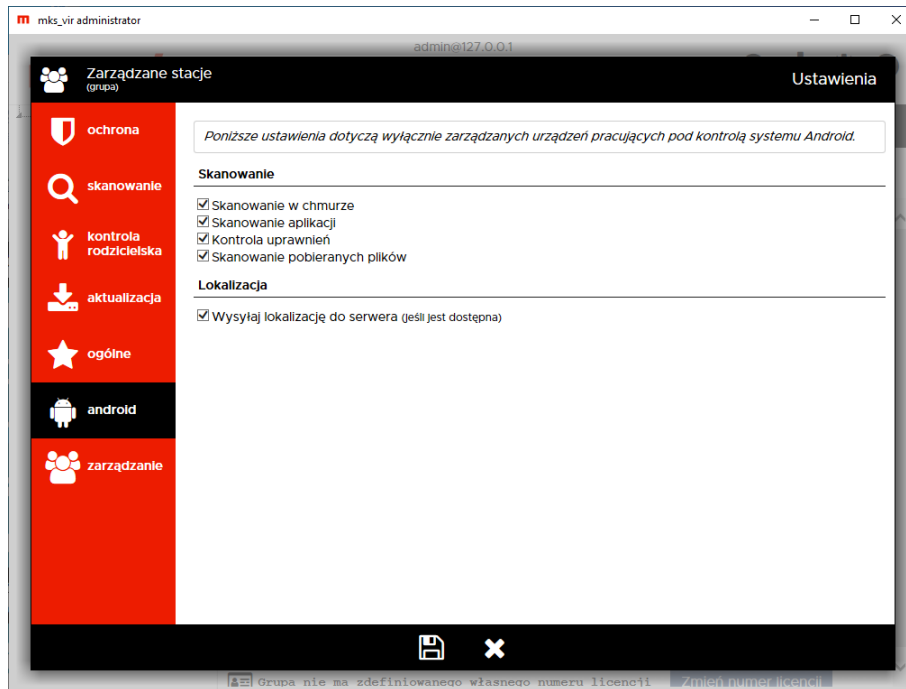


- **Ustawienia użytkownika** – informacja pojawiająca się w przypadku, gdy aktualna konfiguracja programu **mks_vir** nie odpowiada żadnemu z predefiniowanych profili



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

Android:



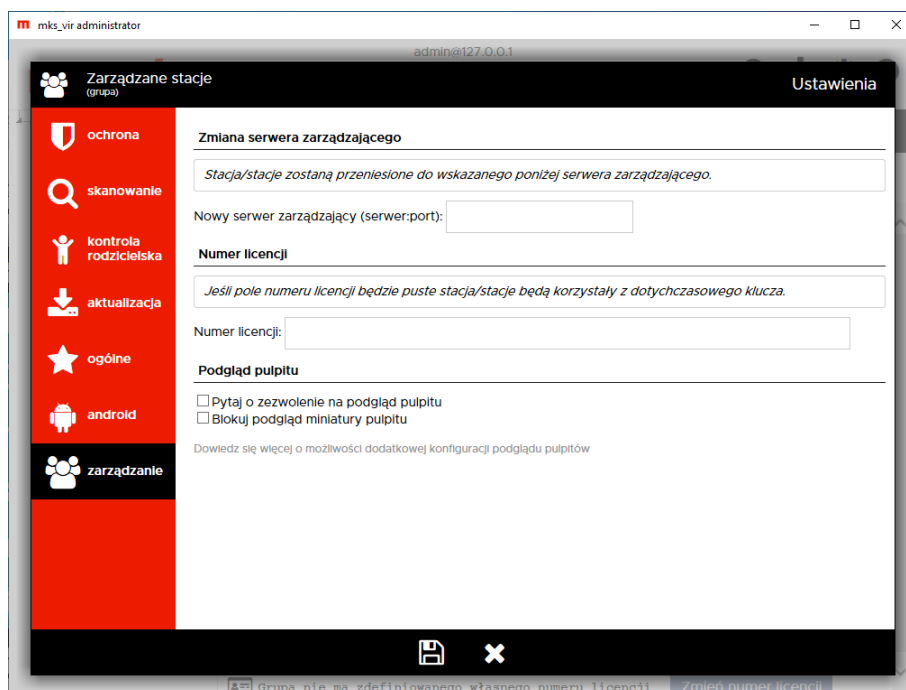
Skanowanie:

- **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

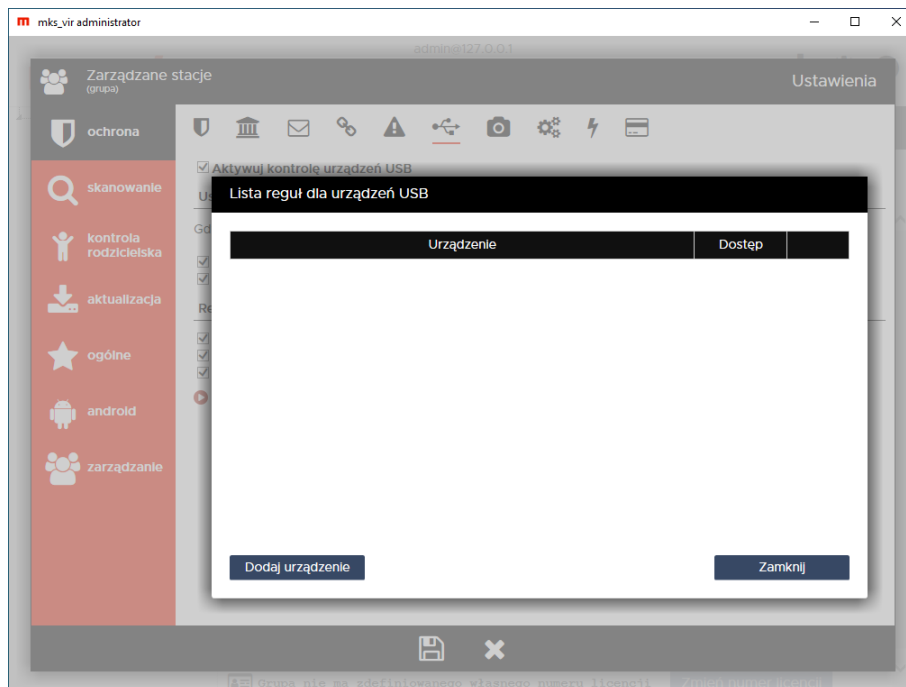
Numer licencji – umożliwia szybką aktualizację/zmianę licencji na stacjach

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

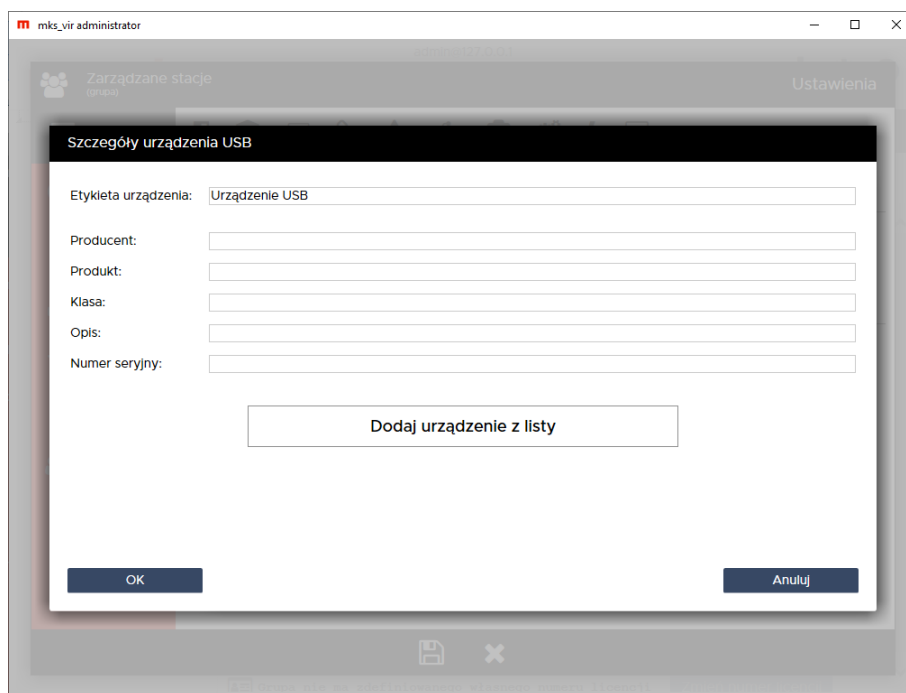
- **Pytaj o zezwolenie na podgląd pulpitu** – umożliwia określenie, czy w przypadku wybrania podglądu pulpitu dla stacji użytkownik ma być pytany o zgodę, czy nie
- **Blokuj podgląd miniatury pulpitu** – umożliwia określenie, czy w przypadku wybrania podglądu pulpitu w grupie, podgląd ma być dostępny,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

Dodawanie reguł w module „Kontrola urządzeń USB”

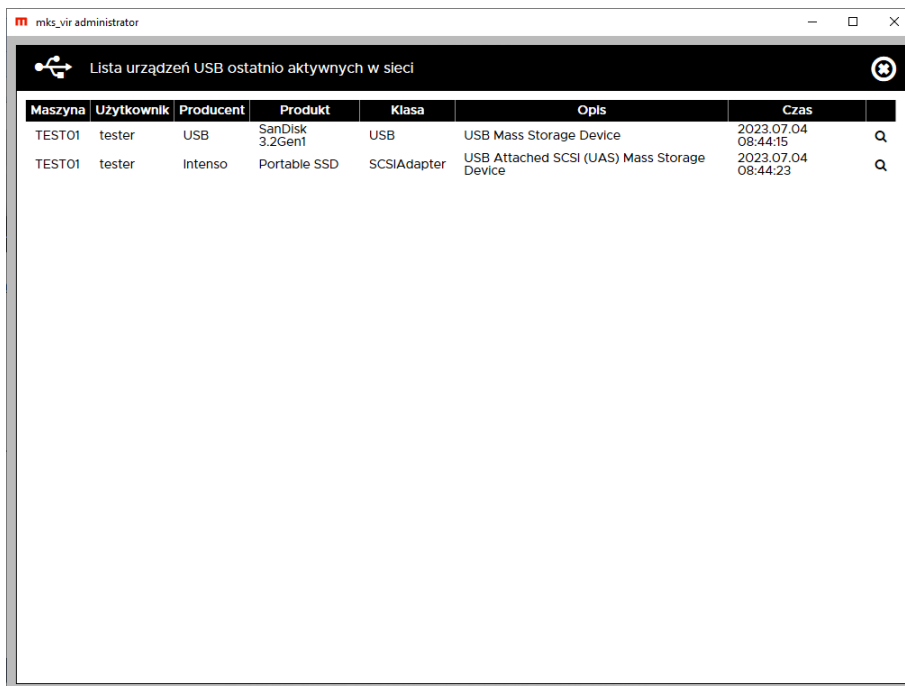
Aby dodać regułę w module „Kontrola urządzeń USB” programu **mks_vir administrator** należy w sekcji ustawień grupy/stacji przejść do „Ochrona → Urządzenia → Pokaż listę reguł dla urządzeń USB” i wybrać „Dodaj urządzenie”:



W nowo otwartym oknie można ręcznie zdefiniować regułę lub dodać z listy (tworzonej na podstawie używanych urządzeń USB na podłączonych stacjach):



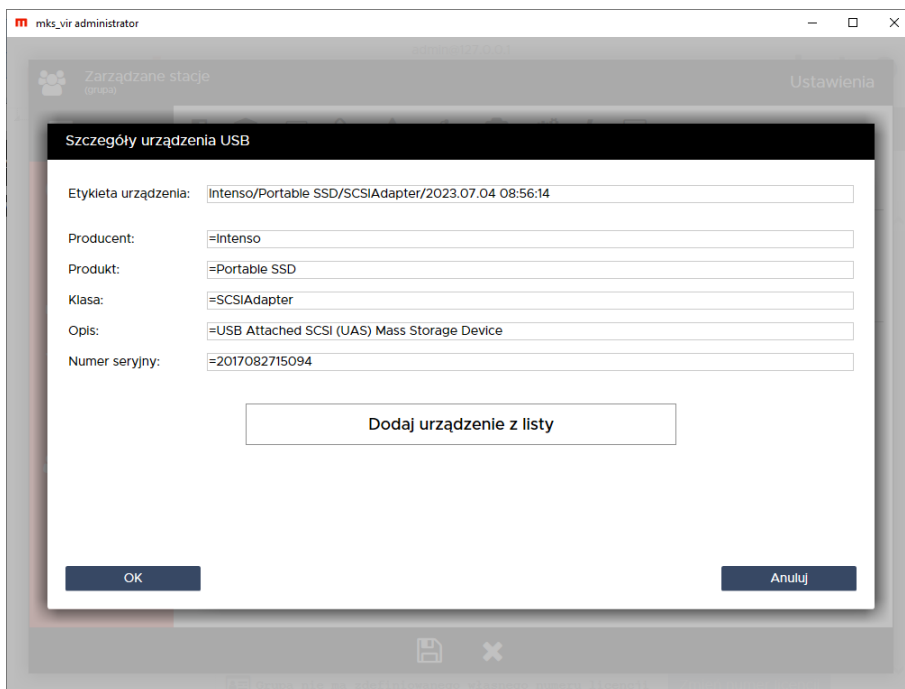
Po wybraniu „Dodaj urządzenie z listy” otwiera się „Lista urządzeń USB ostatnio aktywnych w sieci”:



Lista urządzeń USB ostatnio aktywnych w sieci

Maszyna	Użytkownik	Producent	Produkt	Klasa	Opis	Czas	
TEST01	tester	USB	SanDisk 3.2Gen1	USB	USB Mass Storage Device	2023.07.04 08:44:15	🔍
TEST01	tester	Intenso	Portable SSD	SCSIAdapter	USB Attached SCSI (UAS) Mass Storage Device	2023.07.04 08:44:23	🔍

Wybranie z listy konkretnego urządzenia USB otwiera wypełnione okno definiujące regułę dla tego urządzenia; wciskając „OK” dodajemy regułę do ustawień (po ew. modyfikacji reguły lub bez zmian):



Zarządzane stacje (grupa) Ustawienia

Szczegóły urządzenia USB

Etykieta urządzenia:

Producent:

Produkt:

Klasa:

Opis:

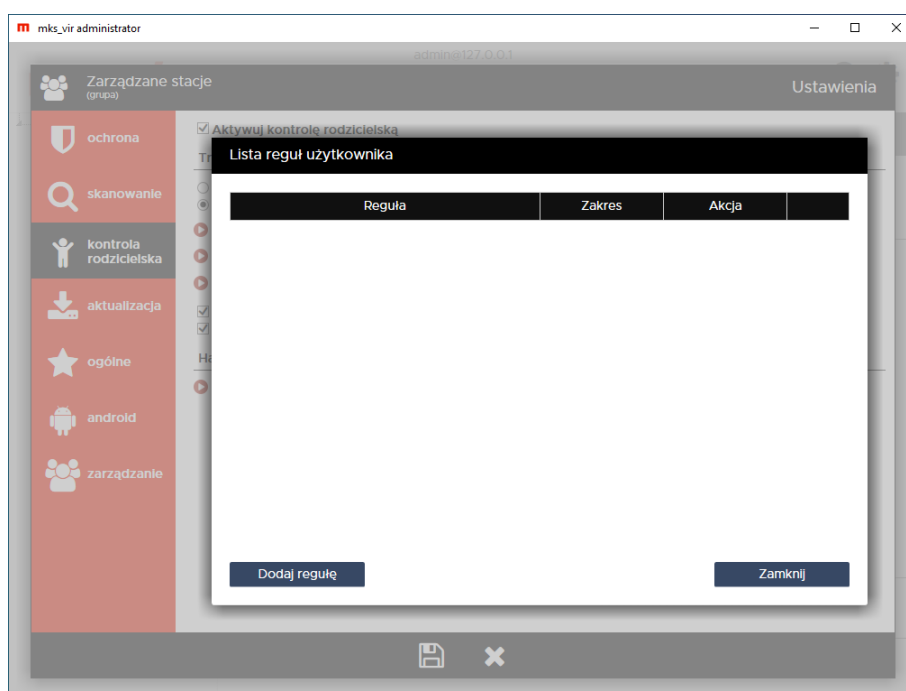
Numer seryjny:

Znak „=” na początku każdego pola reguły (oprócz pola „Etykieta urządzenia”, które jest tylko opisem nie mającym dla działania reguły żadnego znaczenia) powoduje, że zawartość danego pola musi być identyczna z zawartością odpowiedniego pola podłączanego urządzenia, by reguła zadziałała

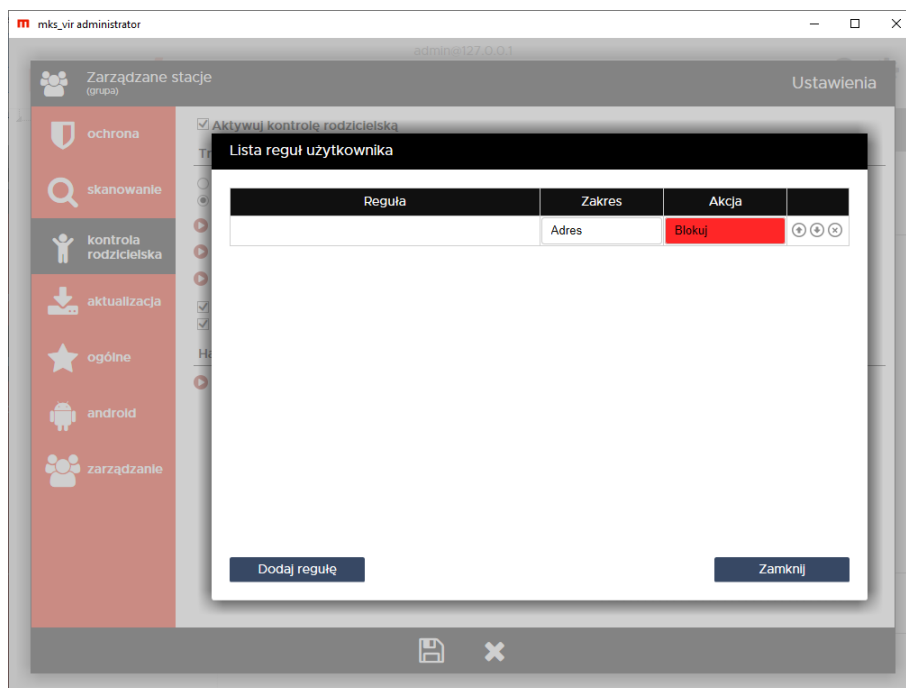
Tworzenie i modyfikacja reguł użytkownika w module „Kontrola rodzicielska”

Uwaga! Aby tworzone lub modyfikowane reguły w module „Kontrola rodzicielska” działały, moduł ten należy uprzednio aktywować w programie **mks_vir administrator**.

W module „Kontrola rodzicielska” jest możliwość definiowania własnych reguł filtrujących dla przeglądanych stron www. Aby utworzyć lub zmodyfikować własne reguły w tym module programu **mks_vir administrator** należy w sekcji ustawień grupy/stacji przejść do „Kontrola rodzicielska → Pokaż listę reguł użytkownika”:



Aby utworzyć własną regułę należy wybrać „Dodaj regułę”, pojawi się wtedy możliwość wpisania własnych definicji, dla których otwierane strony www mają być analizowane i zależnie od tego przepuszczane lub blokowane:



Definicje wpisujemy w polach kolumny „Reguła”, w kolumnie „Zakres” określamy obszar działania danej reguły:

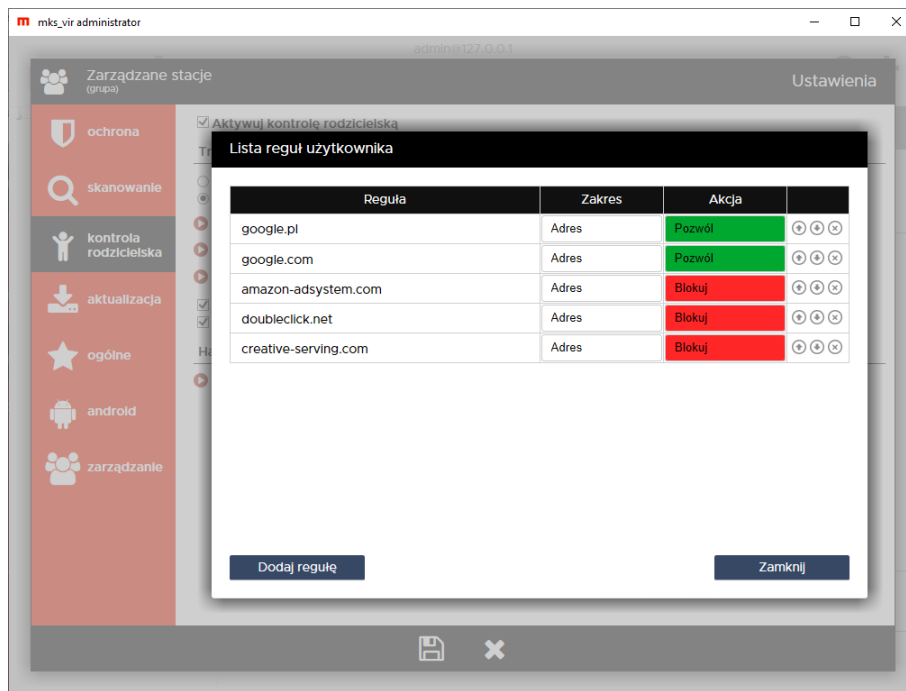
- **Adres** – reguła będzie działała tylko w obszarze adresu otwieranej strony www
- **Treść** – reguła będzie działała tylko w obszarze zawartości otwieranej strony www
- **Wszędzie** – reguła będzie działała zarówno w obszarze adresu, jak i w obszarze zawartości otwieranej strony www

zaś w kolumnie „Akcja” określamy sposób działania danej reguły:

- **Blokuj** – zadziałanie reguły spowoduje zablokowanie otwieranej strony www
- **Pozwól** – zadziałanie reguły spowoduje przepuszczenie otwieranej strony www

Kolejność rozmieszczenia reguł ma znaczenie dla ich działania. Reguły są wykonywane od góry do dołu, czyli jeśli dla otwieranej strony www zadziała jakaś reguła, to następne w kolejności nie będą już dla niej stosowane. Kolejność zdefiniowanych reguł można zmieniać za pomocą strzałek ↑ i ↓ (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak ⊗ (również po prawej stronie).

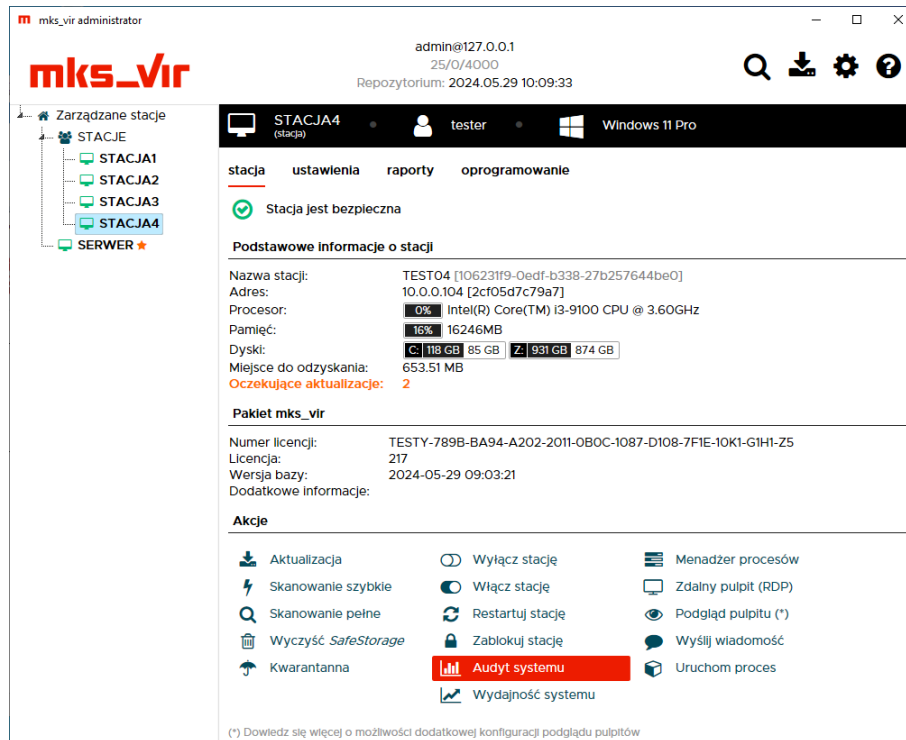
Przykładowa lista zdefiniowanych własnych reguł może wyglądać następująco:



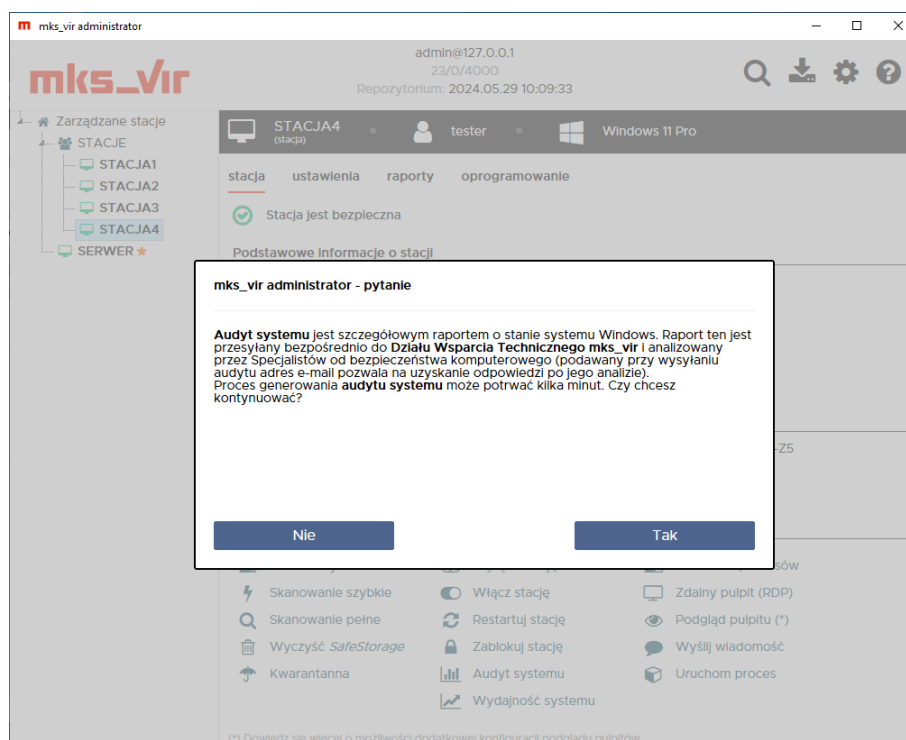
Jak utworzyć i wysłać audyt systemu z konsoli

Aby utworzyć i wysłać do analizy audyt systemu programu **mks_vir** z poziomu konsoli administracyjnej programu **mks_vir administrator** należy posłużyć się poniższą instrukcją:

1. logujemy się w konsoli administracyjnej programu **mks_vir administrator** i zaznaczamy stację dla której chcemy utworzyć audyt systemu:

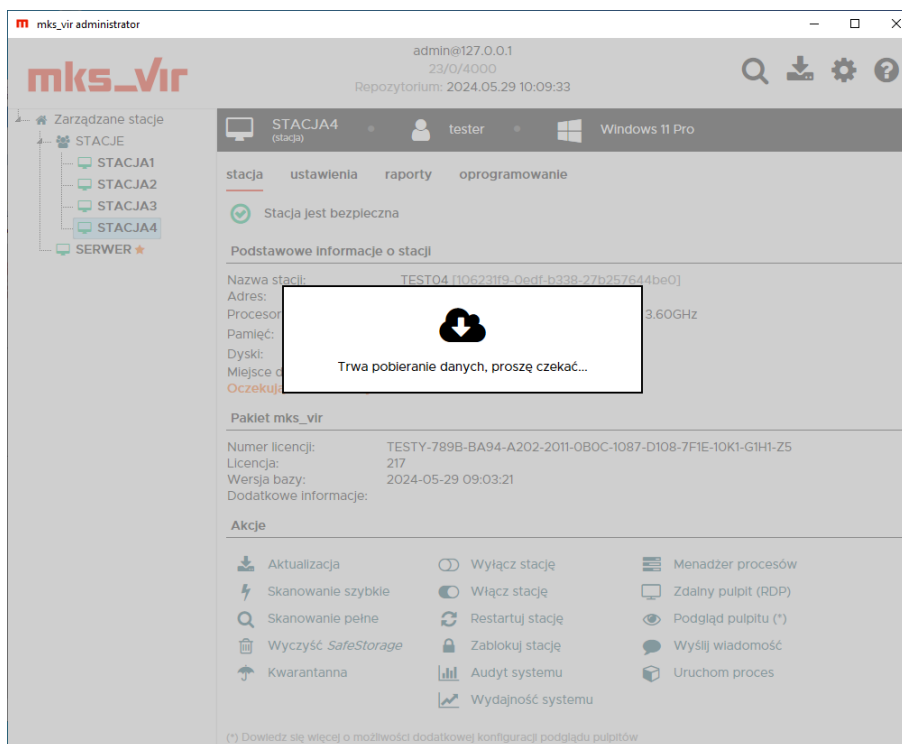


2. wybieramy „Audyt systemu”:



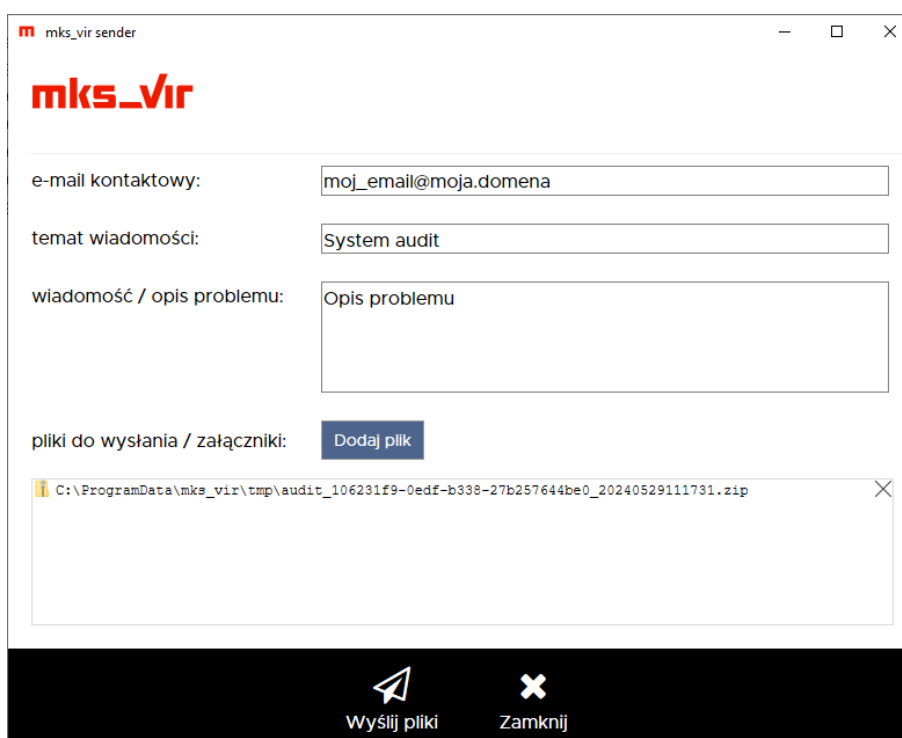
i klikamy „Tak”

3. czekamy aż audyt systemu zostanie pobrany ze stacji:



4. po pobraniu audytu systemu pojawi się formularz do wysłania go; wypełniamy wszystkie trzy pola wpisując:

- w pole „e-mail kontaktowy” swój adres email
- w pole „temat wiadomości” wpisując temat
- w polu „wiadomość/opis problemu” opisując pokrótce problem

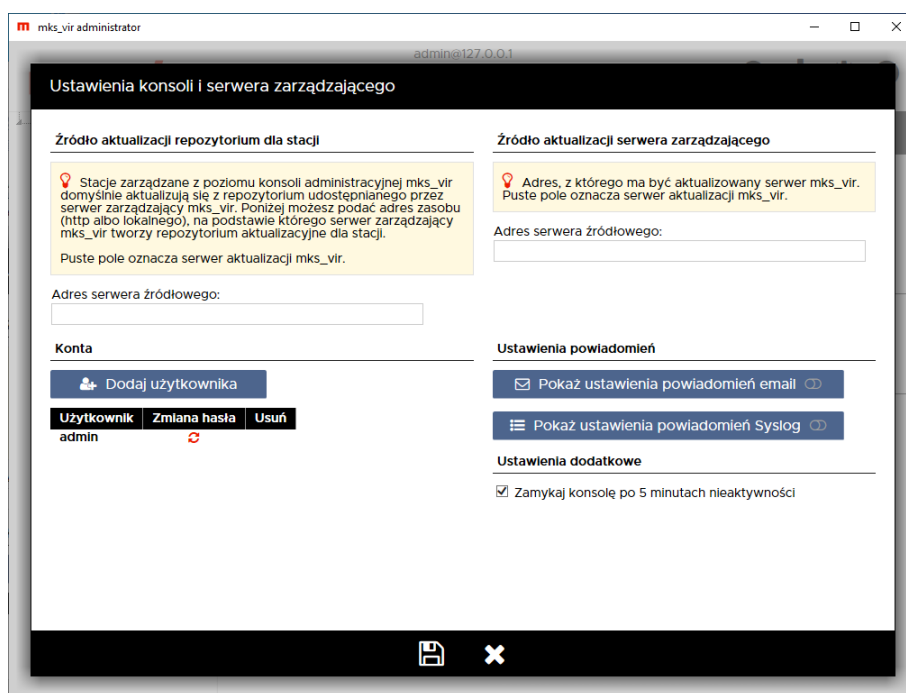


po czym wybieramy „Wyślij pliki”

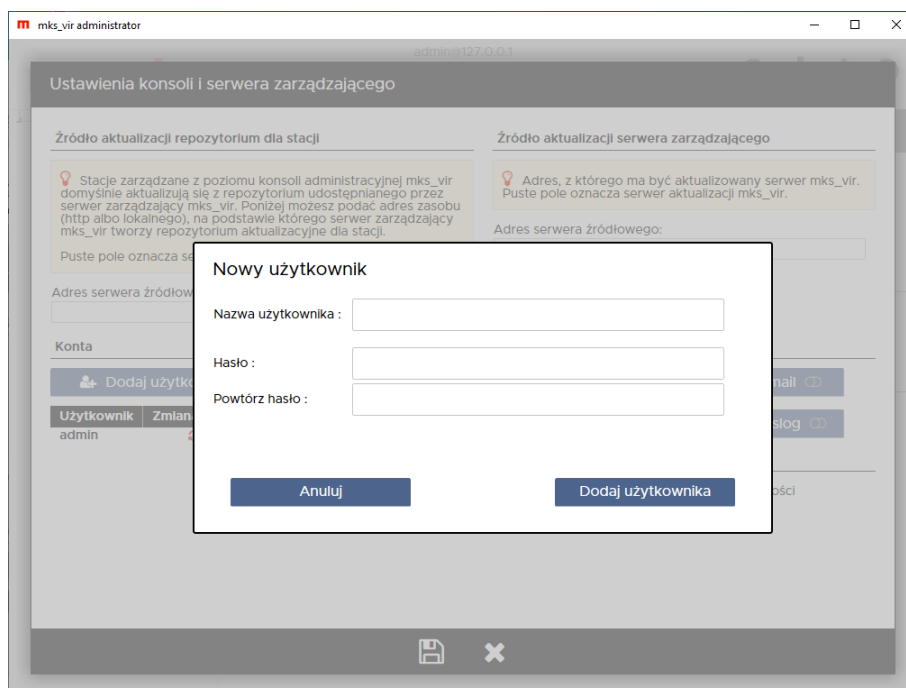
Zarządzanie uprawnieniami

Możliwość modyfikacji praw dostępu do grup dla różnych zdefiniowanych w ustawieniach konsoli i serwera zarządzającego użytkowników ma znaczenie wtedy, gdy kilku różnych administratorów ma mieć możliwość zarządzania tylko niektórymi stacjami rozmieszczonymi w zdefiniowanych uprzednio grupach. Takie prawa dostępu może nadawać i ew. modyfikować główny administrator – użytkownik **admin**.

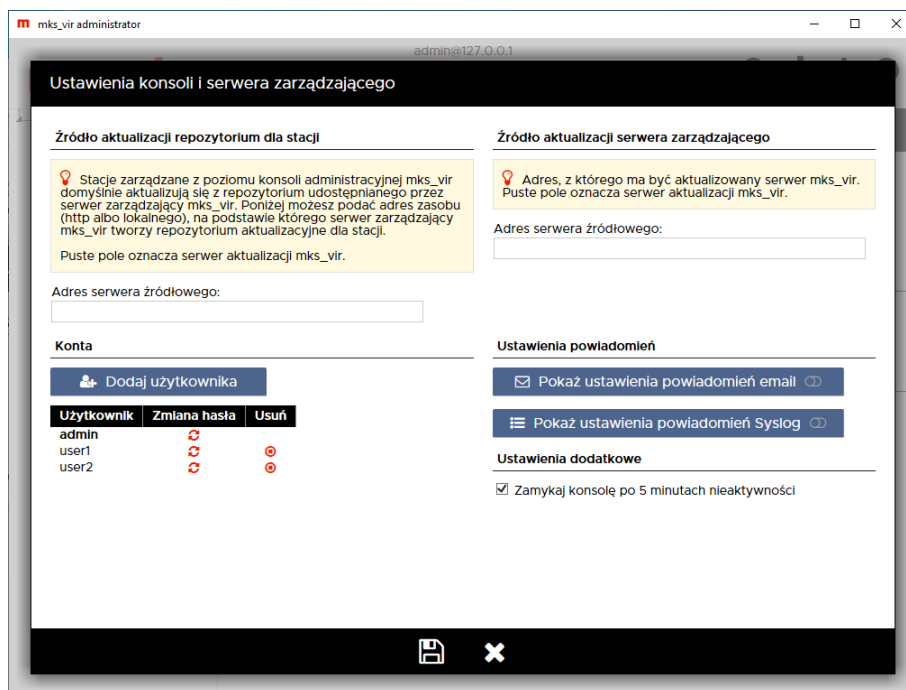
Aby móc modyfikować prawa dostępu dla różnych użytkowników w programie **mks_vir administrator**, należy takich użytkowników utworzyć (prawo tworzenia nowych użytkowników ma tylko użytkownik **admin**). W tym celu należy w konsoli wybrać jej ustawienia (⚙️ w prawym górnym rogu okna konsoli):



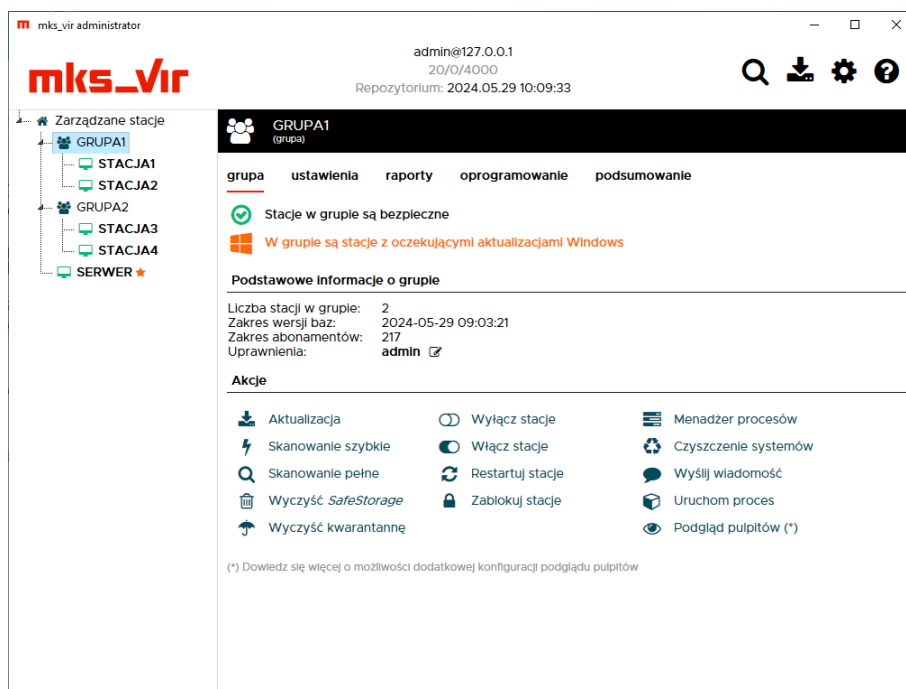
po czym kliknąć w „Dodaj użytkownika”:



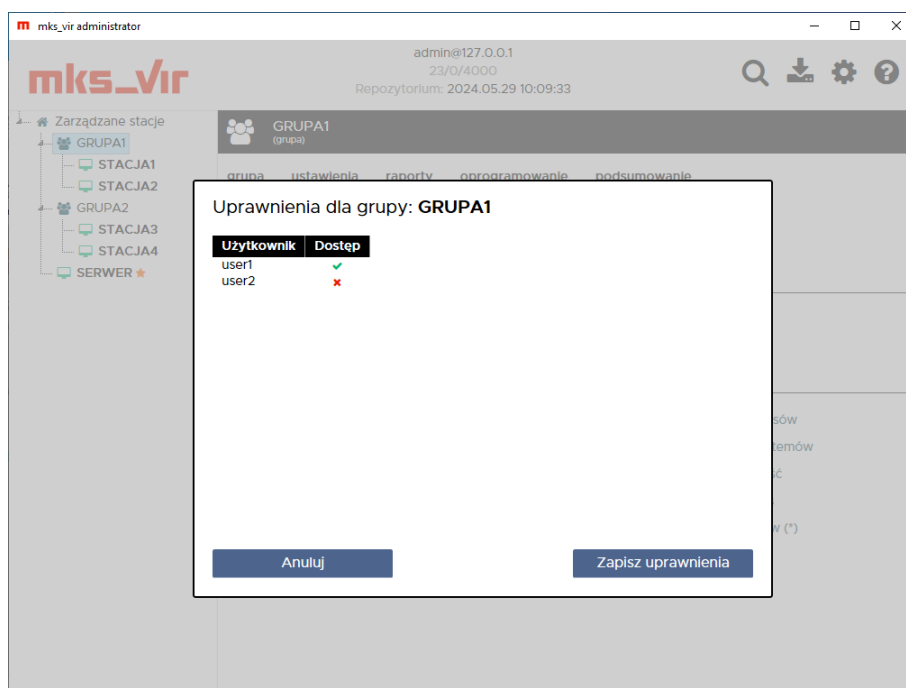
gdzie podajemy nazwę tworzonego użytkownika oraz jego hasło dostępowe – definiujemy w ten sposób tyłu użytkowników, ilu jest potrzebnych:



Aby nadać lub zmodyfikować w konsoli administracyjnej **mks_vir administrator** prawa dostępu należy wybrać grupę, będąc zalogowanym jako użytkownik **admin**, której uprawnienia chcemy zmodyfikować:

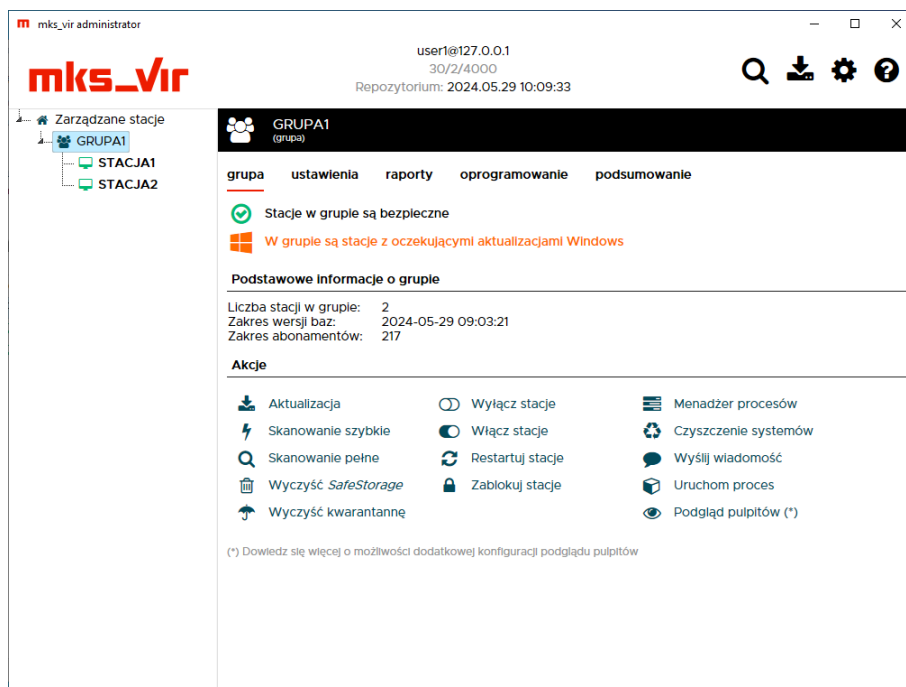


po czym kliknąć ikonę  w linii „Uprawnienia”:

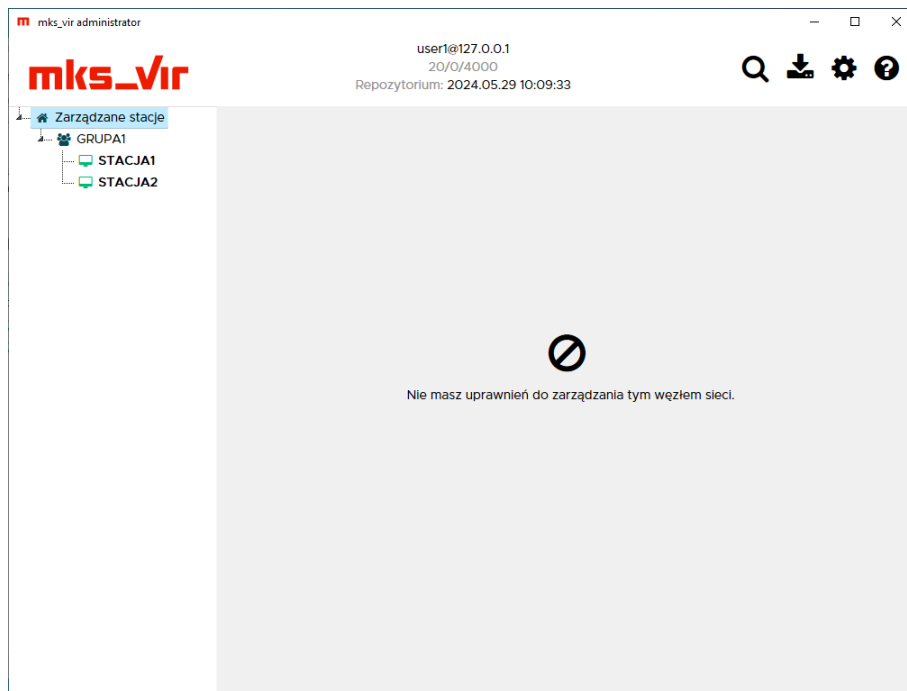


Klikając w ikonki w kolumnie „Dostęp” możemy przydzielać prawo dostępu do danej grupy (✓) lub je odbierać (✗) dla poszczególnych użytkowników. Operację tę powtarzamy dla każdej grupy, której uprawnienia chcemy zmodyfikować.


Po zalogowaniu do konsoli zarządzającej za pomocą użytkownika innego niż **admin** widoczne będą te grupy, do których dany użytkownik ma przydzielone prawa dostępu:

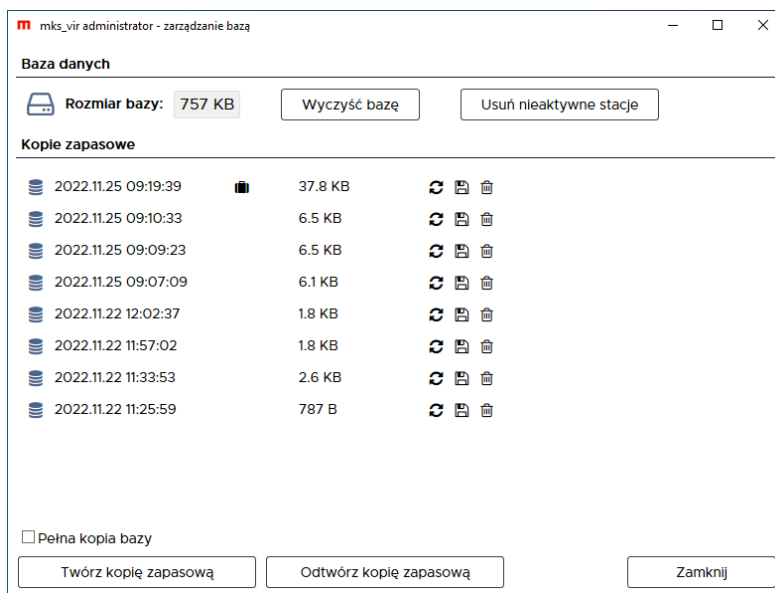


W przypadku braku dostępu do widocznej grupy (może tak zdarzyć się przy bardziej skomplikowanych drzewach grup, a także jak w przykładzie dla grupy „Zarządzane stacje”) wyświetlany będzie odpowiedni komunikat:



Zarządzanie bazą

Moduł **mks_vir administrator – zarządzanie bazą** służy do obsługi bazy danych programu **mks_vir administrator**. Jego głównym zadaniem jest automatyczne tworzenie kopii zapasowych bazy danych, jak również możliwość odtworzenia bazy z takich kopii zapasowych. Aby wywołać moduł zarządzania bazą należy kliknąć prawym klawiszem myszy w ikonę  programu **mks_vir administrator** i wybrać „Zarządzanie bazą”.

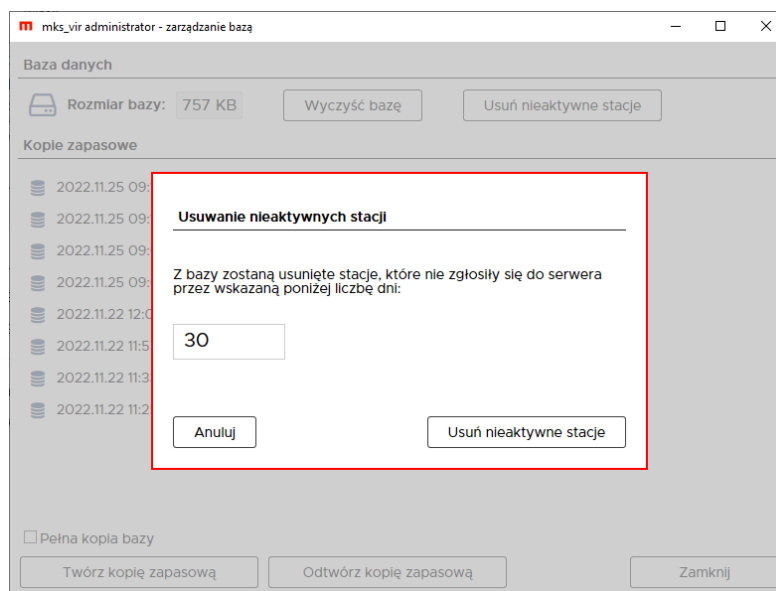


Baza danych:

- **Rozmiar bazy** – podaje aktualną wielkość bazy danych programu **mks_vir administrator**

wybranie „Wyczyść bazę” powoduje usunięcie z bazy danych programu **mks_vir administrator** wszystkich przechowywanych w niej raportów – po takiej operacji nie będzie dostępu do archiwalnych raportów pobranych ze stacji


wybranie „Usuń nieaktywne stacje” powoduje usunięcie z bazy danych programu **mks_vir administrator** wszystkich stacji, które nie zgłaszały się (czyli były nieaktywne) nie krócej niż przez wybraną liczbę dni (domyślnie jest to 30 dni i nie mniej niż 1 dzień)



Kopie zapasowe:

Lista wyświetla aktualnie dostępne kopie zapasowe bazy danych programu **mks_vir administrator** – przechowywane jest maksymalnie 20 ostatnich kopii zapasowych bazy. Na liście są informacje o dokładnym czasie wykonania danej kopii zapasowej, jej wielkość oraz ikonki pozwalające na odtworzenie bazy danych kopii zapasowej, zapisanie kopii zapasowej do pliku i skasowanie danej kopii zapasowej.

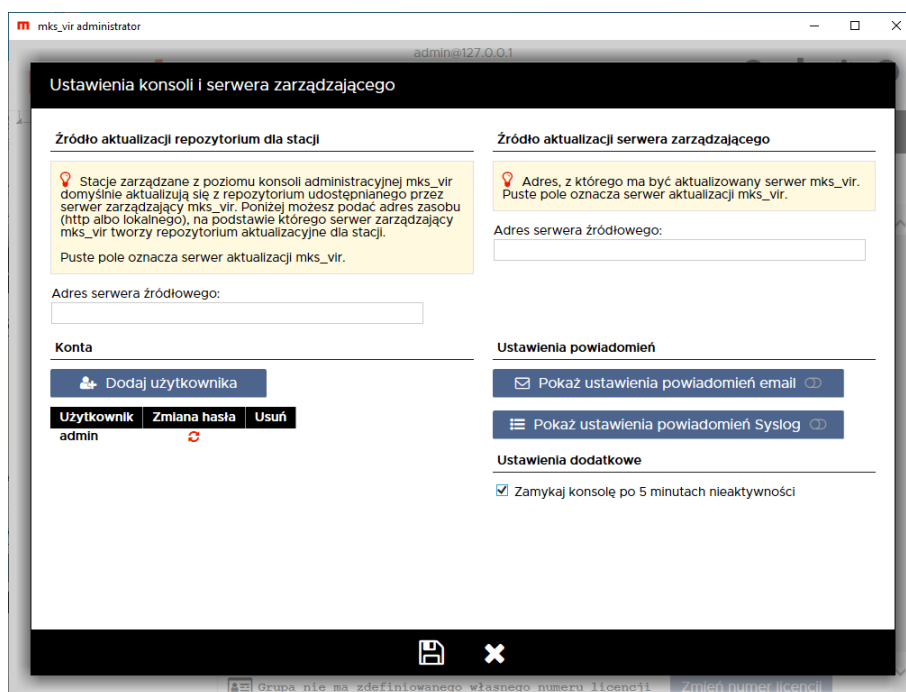
Automatycznie kopie zapasowe bazy danych programu **mks_vir administrator** wykonywane są mniej więcej raz na dobę i zawierają tylko strukturę bazy danych, bez raportów zbieranych ze stacji. Kopię zapasową bazy danych można także wykonać ręcznie wybierając na dole „Twórz kopię zapasową”.

Pełną kopię zapasową bazy danych programu **mks_vir administrator** można wykonać tylko ręcznie, zaznaczając na dole opcję „*Pełna kopia bazy*” i wybierając „Twórz kopię zapasową” – tak wykonana kopia zapasowa jest oznaczana na liście ikoną .

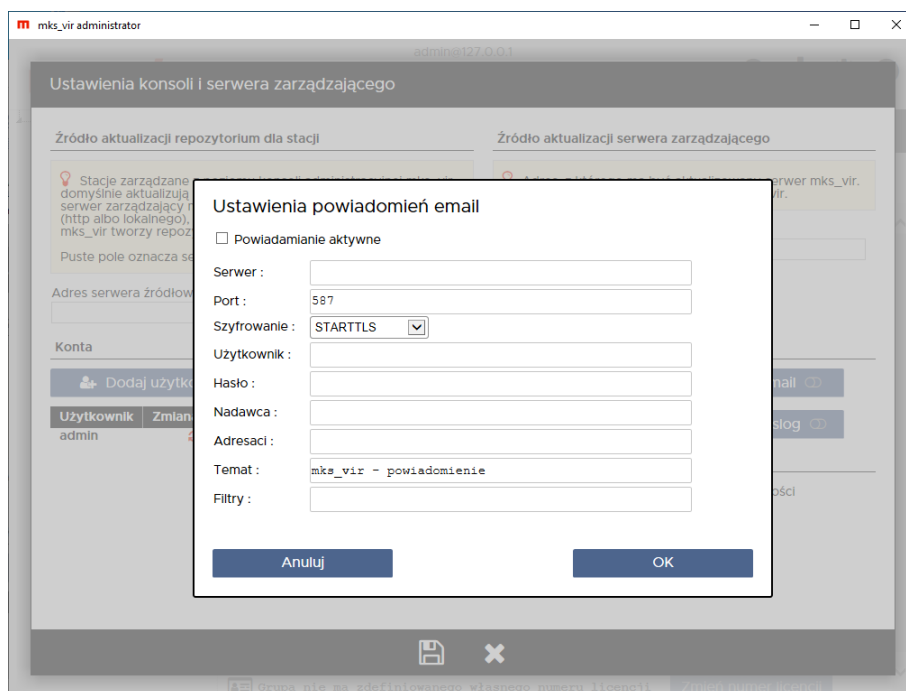
Wybranie „Odtwórz kopię zapasową” pozwala na odtworzenie bazy danych programu **mks_vir administrator** z zewnętrznego pliku kopii zapasowej.

Ustawianie powiadomień email

Aby ustawić w programie **mks_vir administrator** wysyłanie powiadomień email o różnych zdarzeniach występujących na stacjach (przede wszystkim o infekcjach), należy w konsoli wybrać jej ustawienia (⚙️ w prawym górnym rogu okna konsoli), po czym kliknąć w „Pokaż ustawienia powiadomień email”:



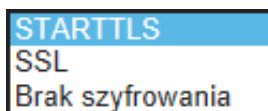
Uruchomi się okno konfiguracji powiadomień:



gdzie należy zaznaczyć opcję „Powiadomienie aktywne” i wypełnić wszystkie pola:

- **Serwer** – adres wykorzystywanego serwera SMTP

- **Port** – port komunikacyjny wykorzystywanego serwera SMTP
- **Szyfrowanie** – rozwijamy i wybieramy odpowiednią opcję, zależnie od rodzaju transmisji danych wymaganych przez serwer SMTP



- **Użytkownik** – nazwa użytkownika wymagana przy autoryzacji wysyłania wiadomości email przez serwer SMTP
- **Hasło** – hasło wymagane przy autoryzacji wysyłania wiadomości email przez serwer SMTP
- **Nadawca** – adres email, który będzie widoczny jako nadawca powiadomienia
- **Adresaci** – adresy email, na które zostanie wysłane powiadomienie; adresy email rozdzielamy przecinkami (w przypadku gdy konieczne jest podanie więcej niż jednego adresu email)
- **Temat** – tekst, który będzie widoczny jako temat powiadomienia
- **Filtry** – definicje rodzajów wysyłanych powiadomień

aby umożliwić wysyłanie powiadomień o danych zdarzeniach, należy wpisać w tym polu kody zdarzeń, o których chcemy otrzymywać powiadomienia (powiadomienia o wykrytych zagrożeniach są wysyłane także w przypadku, gdy lista jest pusta), wpisywane kody oddzielamy spacjami

poniżej lista dopuszczalnych kodów:

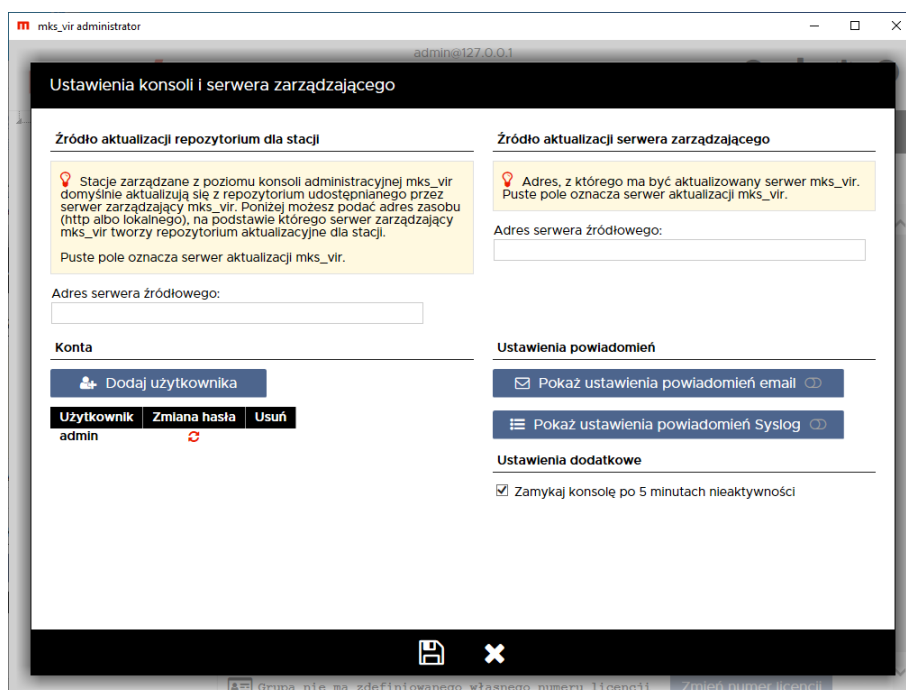
- 0100 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **mks_vir**
- 0101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **mks_vir**
- 0103 – wysłanie powiadomienia w przypadku aktualizacji programu **mks_vir** odroczonej przez użytkownika
- 0301 – wysłanie powiadomienia w przypadku, gdy skanowanie programem **mks_vir** nic nie wykryło
- 0703 – wysłanie powiadomienia w przypadku połączenia zablokowanego przez zaporę programu **mks_vir**
- 0801 – wysłanie powiadomienia w przypadku zakończenia tworzenia kopii zapasowej w programie **mks_vir**
- 1100 – wysłanie powiadomienia w przypadku błędu aktualizacji repozytorium programu **mks_vir administrator**
- 1101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji repozytorium programu **mks_vir administrator**
- 1200 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **mks_vir administrator**
- 1201 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **mks_vir administrator**

- 1401 – wysłanie powiadomienia w przypadku dopuszczenia urządzenia USB przez program **mks_vir**
- 1403 – wysłanie powiadomienia w przypadku zablokowania urządzenia USB przez program **mks_vir**
- 1501 – wysłanie powiadomienia w przypadku dopuszczenia dostępu do urządzenia multimedialnego przez program **mks_vir**
- 1503 – wysłanie powiadomienia w przypadku zablokowania dostępu do urządzenia multimedialnego przez program **mks_vir**
- 1601 – wysłanie powiadomienia w przypadku dopuszczenia aplikacji przez program **mks_vir**
- 1603 – wysłanie powiadomienia w przypadku zablokowania aplikacji przez program **mks_vir**
- 1701 – wysłanie powiadomienia w przypadku zakończenia czyszczenia systemu przez program **mks_vir**
- 1803 – wysłanie powiadomienia w przypadku zmiany sprzętowej w systemie
- 1903 – wysłanie powiadomienia w przypadku problemów z zasobami w systemie (kończące się miejsce na dysku systemowym, problemy sprzętowe zgłaszane do systemu itp.)
- * – wysłanie powiadomienia w przypadku wystąpienia każdego dowolnego zdarzenia (włącza wszystkie filtry)

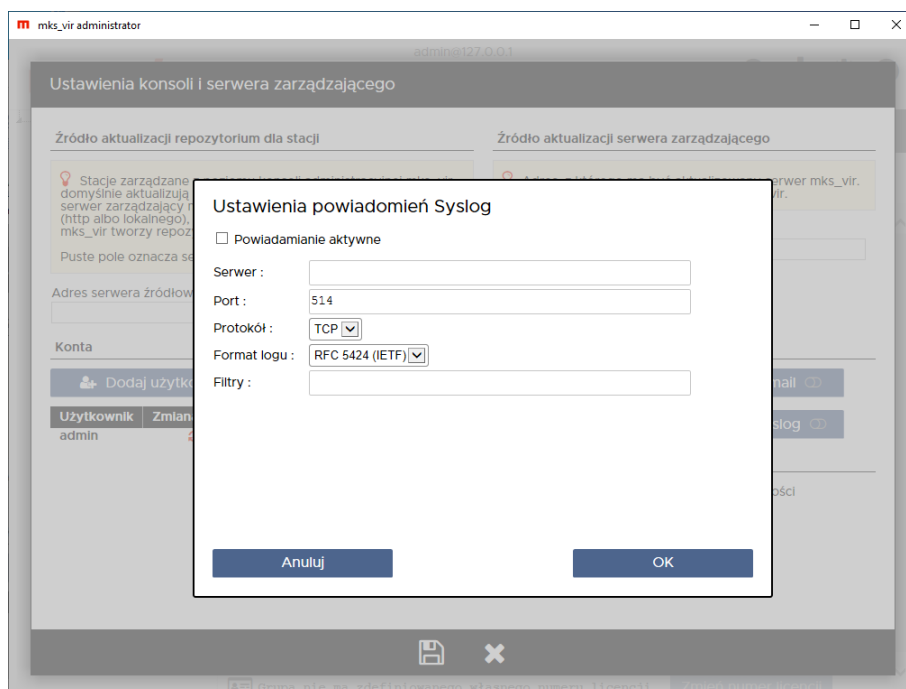
Po poprawnym wypełnieniu wszystkich wymaganych pól zatwierdzamy zmiany przyciskiem „OK”

Ustawianie powiadomień syslog

Aby ustawić w programie **mks_vir administrator** wysyłanie powiadomień do serwerów SYSLOG o różnych zdarzeniach występujących na stacjach (przede wszystkim o infekcjach), należy w konsoli wybrać jej ustawienia (⚙️ w prawym górnym rogu okna konsoli), po czym kliknąć w „Pokaż ustawienia powiadomień Syslog”:



Uruchomi się okno konfiguracji powiadomień:



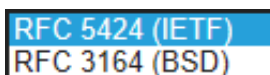
gdzie należy zaznaczyć opcję „Powiadomienie aktywne” i wypełnić wszystkie pola:

- **Serwer** – adres wykorzystywanego serwera SYSLOG

- **Port** – port komunikacyjny wykorzystywanego serwera SYSLOG (domyślnym jest port 514)
- **Protokół** – rozwijamy i wybieramy odpowiednią opcję, zależnie od rodzaju transmisji danych wymaganych przez serwer SYSLOG (protokół TCP lub UDP)



- **Format logu** – rozwijamy i wybieramy odpowiednią opcję, zależnie od rodzaju formatu logów wymaganych przez serwer SYSLOG (format nowszy RFC 5424 lub starszy RFC 3164)



- **Filtry** – definicje rodzajów wysyłanych powiadomień
aby umożliwić wysyłanie powiadomień o danych zdarzeniach, należy wpisać w tym polu kody zdarzeń, o których chcemy otrzymywać powiadomienia (powiadomienia o wykrytych zagrożeniach są wysyłane także w przypadku, gdy lista jest pusta), wpisywane kody oddzielamy spacjami
poniżej lista dopuszczalnych kodów:
 - 0100 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **mks_vir**
 - 0101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **mks_vir**
 - 0103 – wysłanie powiadomienia w przypadku aktualizacji programu **mks_vir** odroczonej przez użytkownika
 - 0301 – wysłanie powiadomienia w przypadku, gdy skanowanie programem **mks_vir** nic nie wykryło
 - 0703 – wysłanie powiadomienia w przypadku połączenia zablokowanego przez zapórę programu **mks_vir**
 - 0801 – wysłanie powiadomienia w przypadku zakończenia tworzenia kopii zapasowej w programie **mks_vir**
 - 1100 – wysłanie powiadomienia w przypadku błędu aktualizacji repozytorium programu **mks_vir administrator**
 - 1101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji repozytorium programu **mks_vir administrator**
 - 1200 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **mks_vir administrator**
 - 1201 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **mks_vir administrator**
 - 1401 – wysłanie powiadomienia w przypadku dopuszczenia urządzenia USB przez program **mks_vir**
 - 1403 – wysłanie powiadomienia w przypadku zablokowania urządzenia USB przez program **mks_vir**

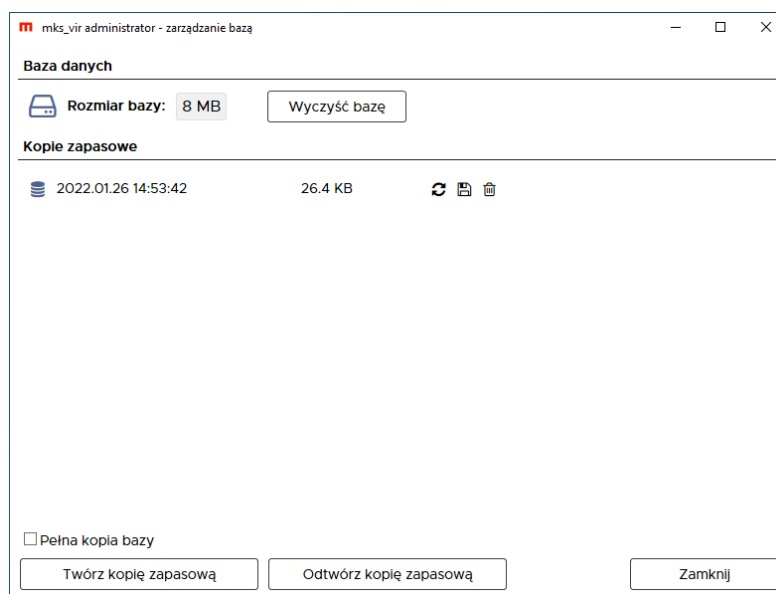
- 1501 – wysłanie powiadomienia w przypadku dopuszczenia dostępu do urządzenia multimedialnego przez program **mks_vir**
- 1503 – wysłanie powiadomienia w przypadku zablokowania dostępu do urządzenia multimedialnego przez program **mks_vir**
- 1601 – wysłanie powiadomienia w przypadku dopuszczenia aplikacji przez program **mks_vir**
- 1603 – wysłanie powiadomienia w przypadku zablokowania aplikacji przez program **mks_vir**
- 1701 – wysłanie powiadomienia w przypadku zakończenia czyszczenia systemu przez program **mks_vir**
- 1803 – wysłanie powiadomienia w przypadku zmiany sprzętowej w systemie
- 1903 – wysłanie powiadomienia w przypadku problemów z zasobami w systemie (kończące się miejsce na dysku systemowym, problemy sprzętowe zgłaszane do systemu itp.)
- * – wysłanie powiadomienia w przypadku wystąpienia każdego dowolnego zdarzenia (włącza wszystkie filtry)

Po poprawnym wypełnieniu wszystkich wymaganych pól zatwierdzamy zmiany przyciskiem „OK”


Jak przeinstalować program mks_vir administrator z zachowaniem ustawień

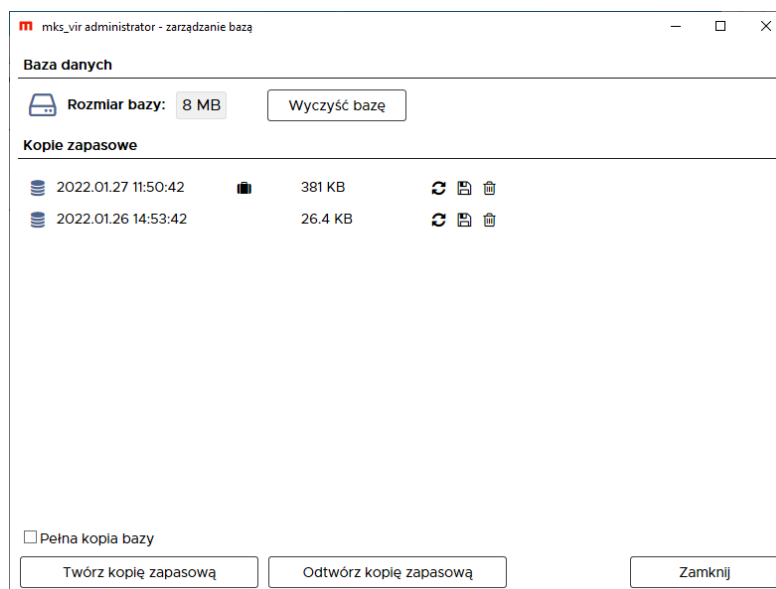
Czasami występuje konieczność reinstalacji systemu Windows (szczególnie w przypadkach zmiany komputera na nowszy) i wszystkich programów w nim zainstalowanych, co może wiązać się z koniecznością ich ponownej konfiguracji. W przypadku programu **mks_vir administrator** można w prosty sposób zachować, a po reinstalacji przywrócić wszelkie ustawienia wprowadzone przez użytkowników zarządzających. W tym celu należy posłużyć się poniższą instrukcją:

1. uruchamiamy program zarządzający bazą **mks_vir administrator** klikając prawym klawiszem myszy w ikonę programu i wybierając „Zarządzanie bazą”:



2. wybieramy „Twórz kopię zapasową”

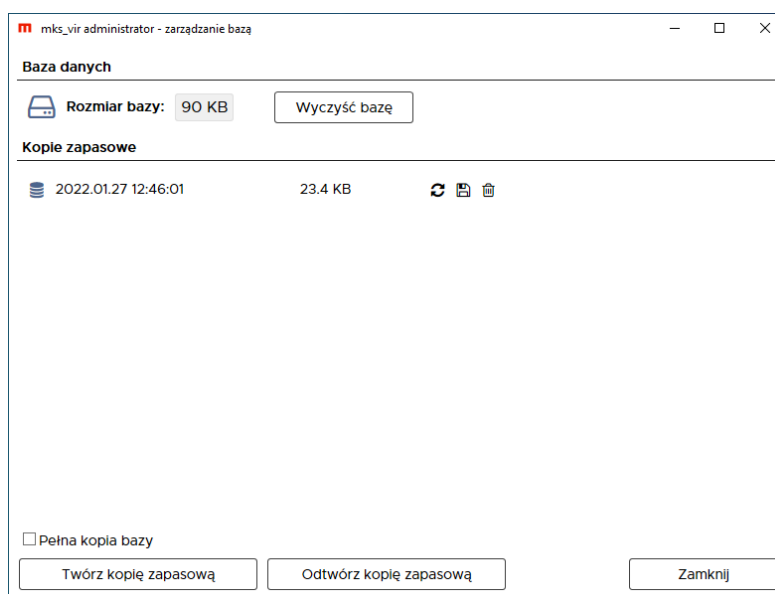
Taka kopia zachowuje tylko ustawienia, ale jeśli zależy nam również na zachowaniu dotychczasowych raportów zebranych z zarządzanych stacji, należy przed jej utworzeniem zaznaczyć opcję „*Pełna kopia bazy*” – wykonana w ten sposób kopia jest oznaczana ikoną :



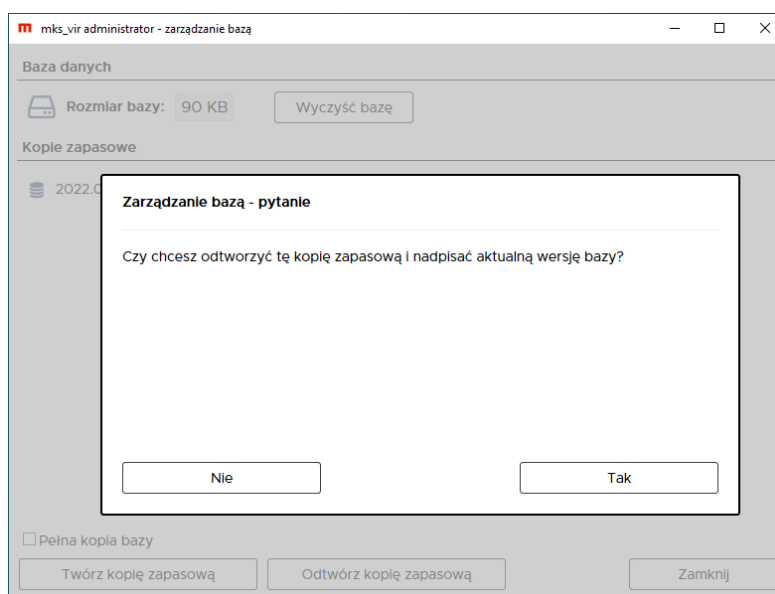
3. tak utworzoną kopię zapasową bazy programu **mks_vir administrator** zapisujemy do pliku klikając w ikonę dyskietki

W nowej instalacji programu **mks_vir administrator** odtwarzamy dotychczasowe ustawienia posługując się poniższą instrukcją:

1. uruchamiamy program zarządzający bazą **mks_vir administrator** klikając prawym klawiszem myszy w ikonę programu i wybierając „Zarządzanie bazą”:



2. wybieramy „Odtwórz kopię zapasową”, wskazujemy wcześniej utworzony plik kopii zapasowej bazy i wybieramy „Otwórz” – pojawi się komunikat o zgodę na nadpisanie aktualnej wersji bazy, należy się na to zgodzić:

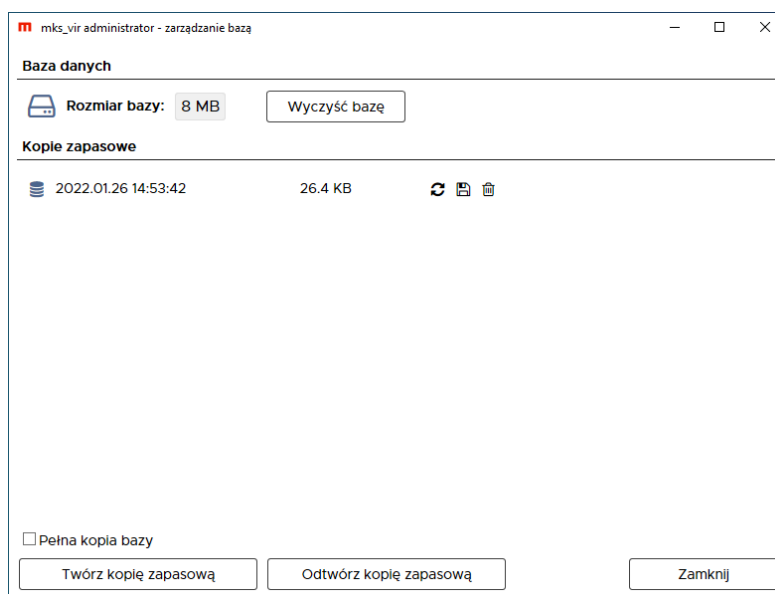


3. po zakończeniu odtwarzania bazy zamykamy program zarządzający bazą

Jak przenieść program mks_vir administrator na inny komputer w sieci z zachowaniem ustawień

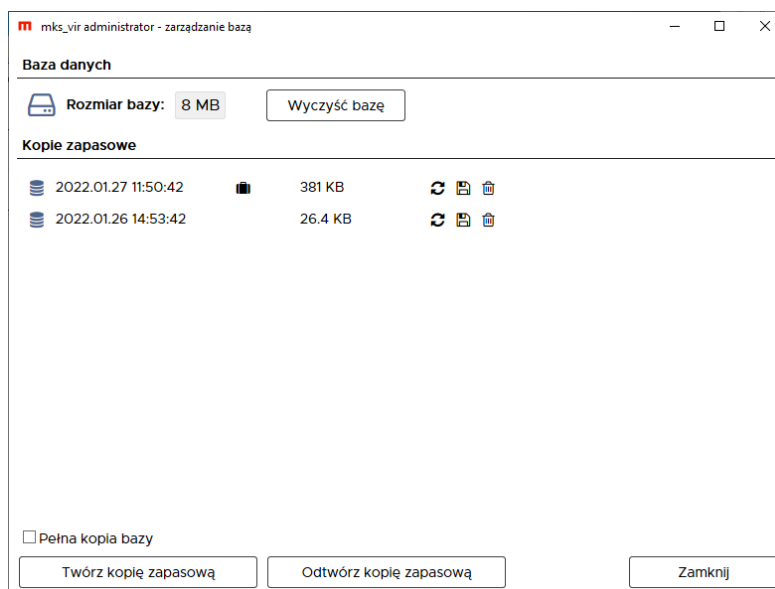
Czasami występuje konieczność przeniesienia programu **mks_vir administrator** na komputer o innym adresie sieciowym i w takim przypadku można w prosty sposób zachować wszelkie ustawienia wprowadzone przez użytkowników zarządzających. W tym celu należy posłużyć się poniższą instrukcją:

1. uruchamiamy program zarządzający bazą **mks_vir administrator** klikając prawym klawiszem myszy w ikonę programu i wybierając „Zarządzanie bazą”:



2. wybieramy „Twórz kopię zapasową”

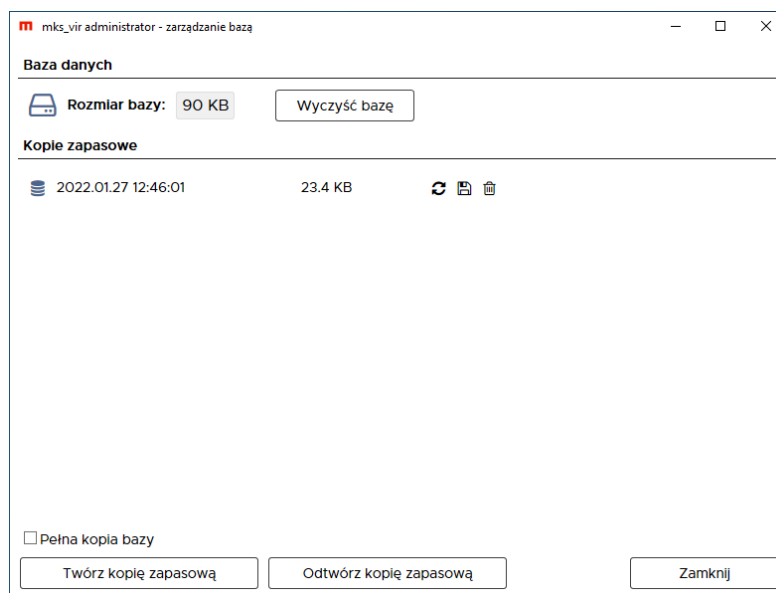
Taka kopia zachowuje tylko ustawienia, ale jeśli zależy nam również na zachowaniu dotychczasowych raportów zebranych z zarządzanych stacji, należy przed jej utworzeniem zaznaczyć opcję „Pełna kopia bazy” – wykonana w ten sposób kopia jest oznaczana ikoną 🗑️:



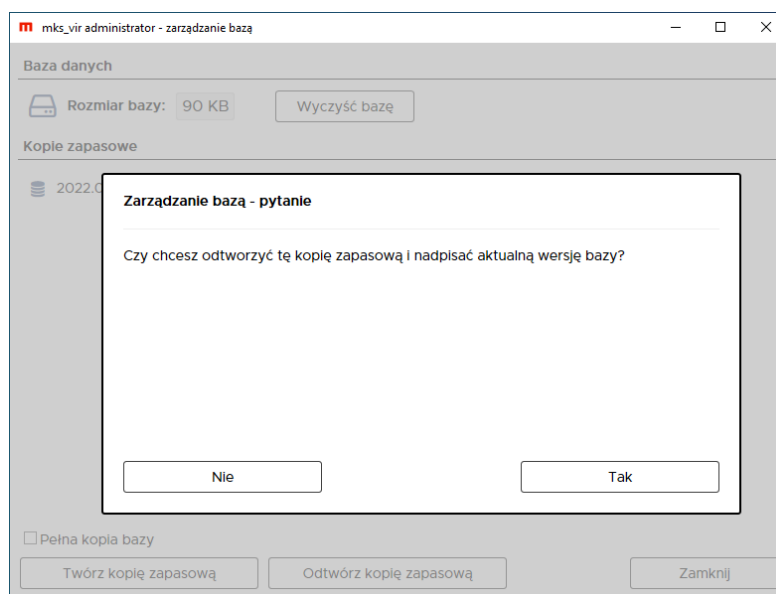
3. tak utworzoną kopię zapasową bazy programu **mks_vir administrator** zapisujemy do pliku klikając w ikonę dyskietki

W nowej instalacji programu **mks_vir administrator** odtwarzamy dotychczasowe ustawienia posługując się poniższą instrukcją:

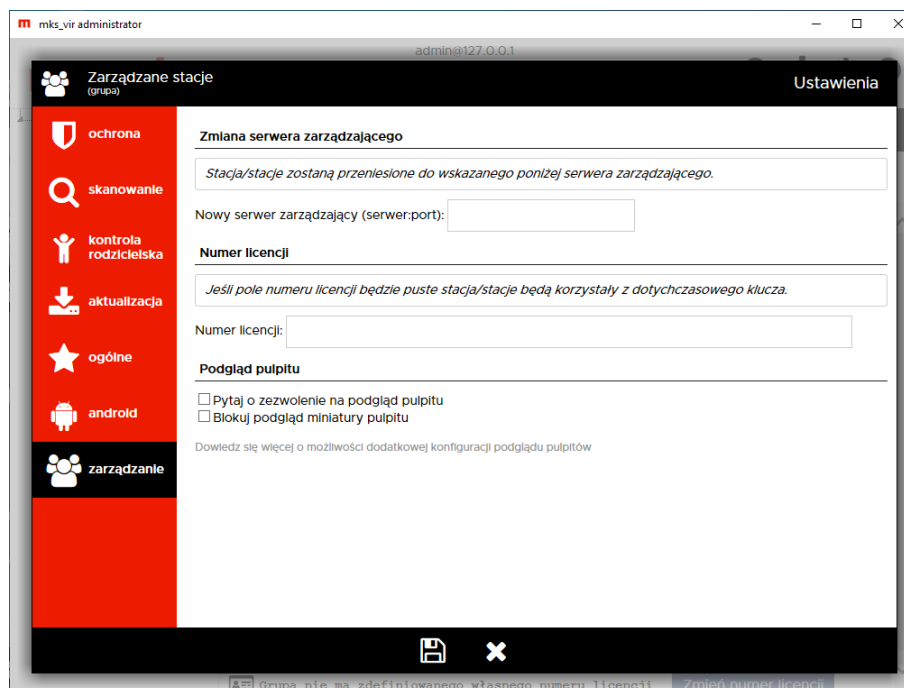
1. uruchamiamy program zarządzający bazą **mks_vir administrator** klikając prawym klawiszem myszy w ikonę programu i wybierając „Zarządzanie bazą”:



2. wybieramy „Odtwórz kopię zapasową”, wskazujemy wcześniej utworzony plik kopii zapasowej bazy i wybieramy „Otwórz” – pojawi się komunikat o zgodę na nadpisanie aktualnej wersji bazy, należy się na to zgodzić:



3. po zakończeniu odtwarzania bazy zamykamy program zarządzający bazą
4. na starym komputerze w programie **mks_vir administrator** ustawiamy adres nowego komputera z zainstalowanym programem **mks_vir administrator**, co wykonuje się w ustawieniach grupy lub stacji, w sekcji „Zarządzanie”:



w polu „Zmiana serwera zarządzającego” podajemy adres sieciowy nowego komputera z zainstalowanym programem **mks_vir administrator**, po czym należy poczekać aż wszystkie stacje **mks_vir** przełączą się do nowego serwera zarządzającego

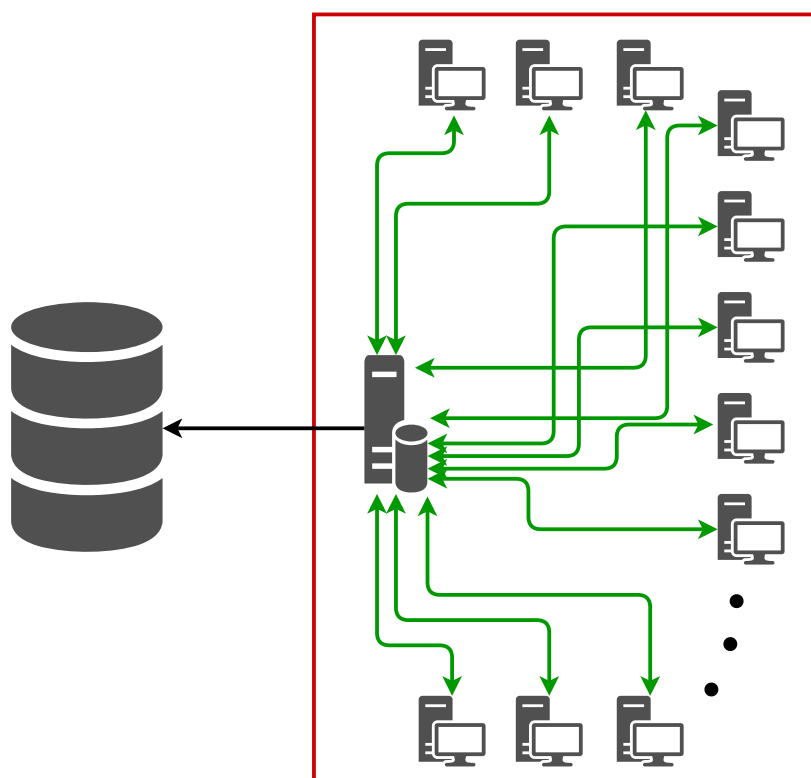
jeśli grupy lub stacje posiadają indywidualne ustawienia, to podanie nowego adresu należy wykonać w każdej takiej oddzielnej konfiguracji

Zalety korzystania z programu mks_vir administrator w sieciach lokalnych (LAN)

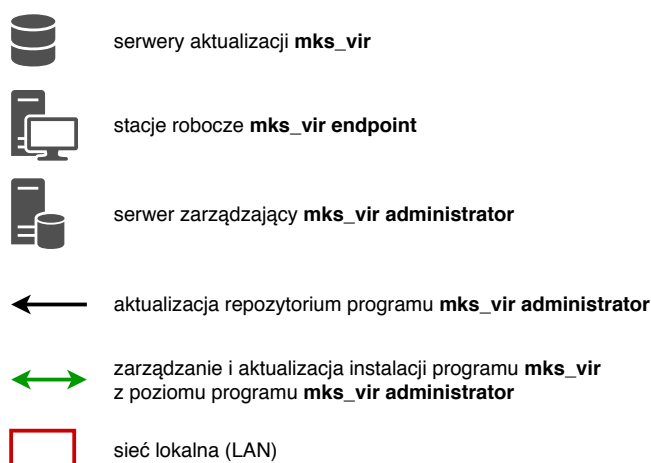
Zarządzanie w sieciach lokalnych (LAN) stacjami z zainstalowanymi programami **mks_vir** z poziomu programu **mks_vir administrator** ma kilka głównych zalet:

1. **centralna aktualizacja** – program **mks_vir administrator** sam tworzy, aktualizuje i udostępnia repozytorium aktualizacyjne dla zainstalowanych na stacjach programów **mks_vir**, dzięki czemu obciążenie łącza internetowego jest niewielkie, a to dlatego, że tylko program **mks_vir administrator** łączy się z *serwerami aktualizacyjnymi mks_vir*
uwaga! w przypadku, gdy komputer pełniący rolę serwera administracyjnego **mks_vir administrator** jest wyłączony, programy **mks_vir** zainstalowane na stacjach aktualizują się bezpośrednio z *serwerów aktualizacyjnych mks_vir*
2. **centralna konfiguracja** – zainstalowane na stacjach programy **mks_vir** konfigurowane są z poziomu konsoli administracyjnej **mks_vir administrator**, dzięki czemu nie trzeba wykonywać tych samych czynności na każdej stacji z osobna – ma to szczególne znaczenie w sieciach lokalnych (LAN) z dużą ilością stacji
uwaga! w przypadku, gdy komputer pełniący rolę serwera administracyjnego **mks_vir administrator** jest wyłączony, nie ma możliwości zmian konfiguracji w programach **mks_vir** zainstalowanych na stacjach
3. **centralny nadzór nad bezpieczeństwem** – z poziomu konsoli administracyjnej **mks_vir administrator** można kontrolować i reagować na potencjalnie pojawiające się zagrożenia na stacjach z zainstalowanym programem **mks_vir** bez konieczności sprawdzania tego na każdej stacji oddzielnie

Można to odzwierciedlić za pomocą poniższego diagramu:

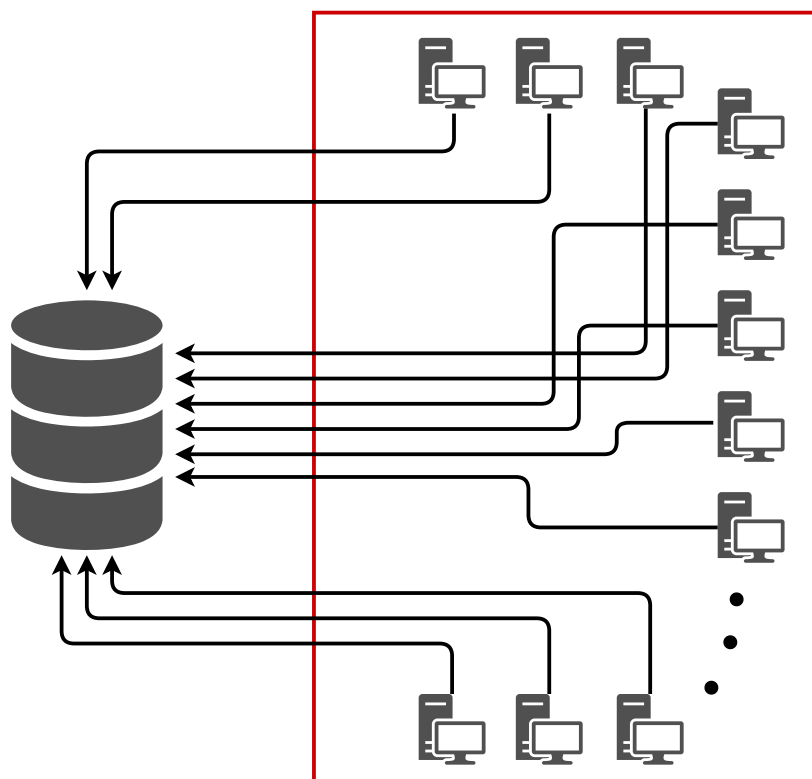


gdzie:

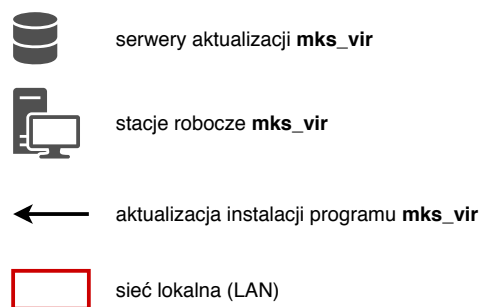


Brak zarządzania z poziomu programu mks_vir administrator

W przypadku sieci lokalnej (LAN) z zainstalowanymi na stacjach programami **mks_vir**, ale bez zarządzania z poziomu programu **mks_vir administrator**, aktualizacja każdego programu **mks_vir** jest realizowana bezpośrednio z serwerów aktualizacyjnych **mks_vir**, co można odzwierciedlić za pomocą poniższego diagramu:



gdzie:



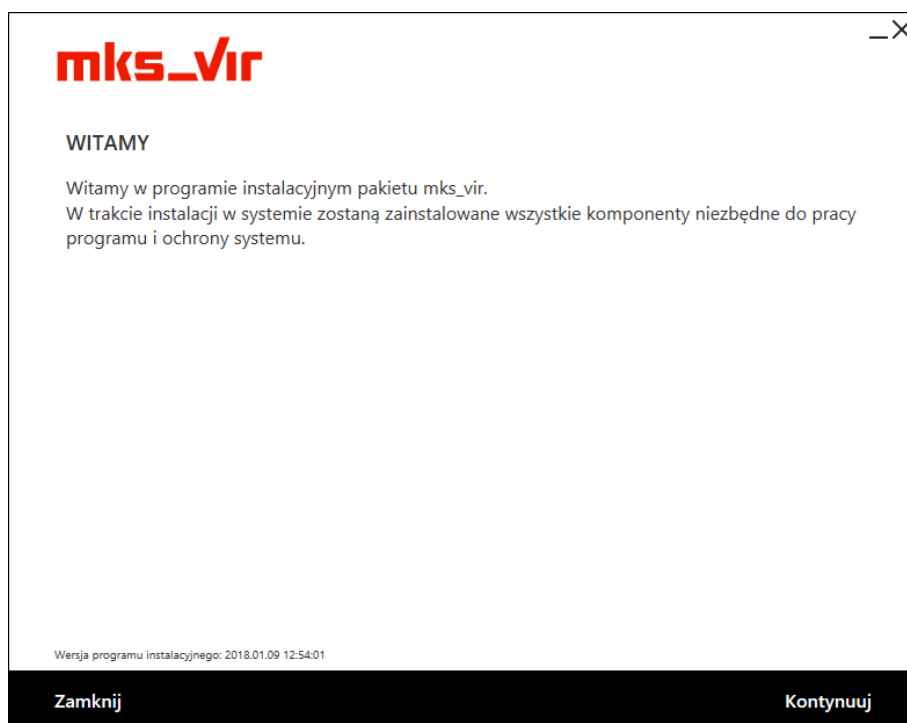
Można zauważyć, że przy dużej ilości stacji w sieci lokalnej (LAN) wymuszenie aktualizacji zainstalowanych programów **mks_vir** mniej więcej w tym samym czasie, może spowodować spore obciążenie łącza internetowego

W tym przypadku również ew. modyfikacje konfiguracji programów **mks_vir** trzeba wykonać na każdej ze stacji oddzielnie.

Instalacja

Instalacja programu mks_vir

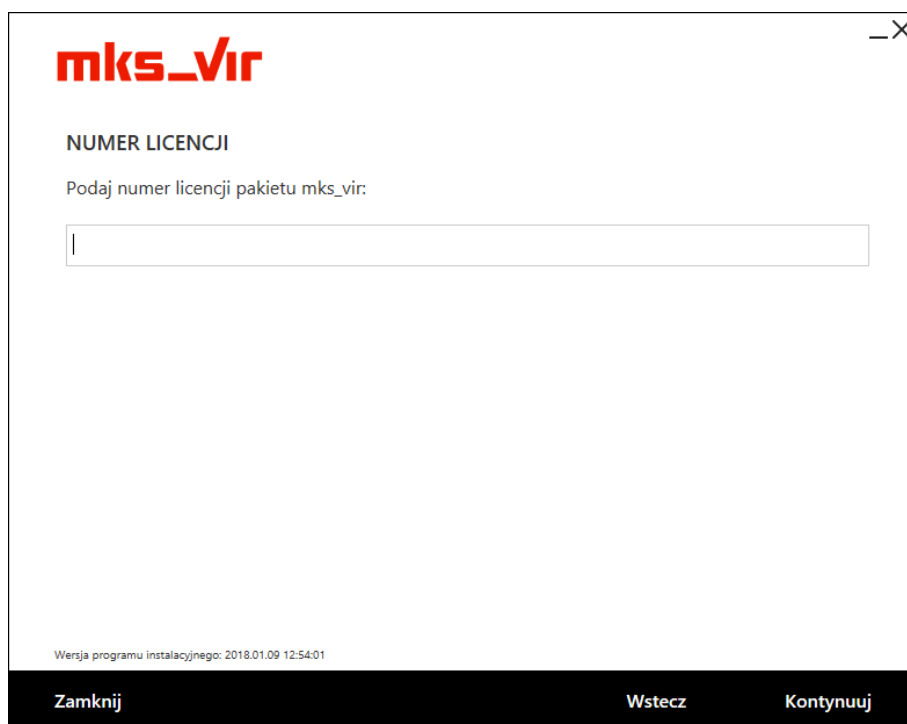
Po uruchomieniu instalatora pojawi się okno dialogowe umożliwiające rozpoczęcie instalacji programu:



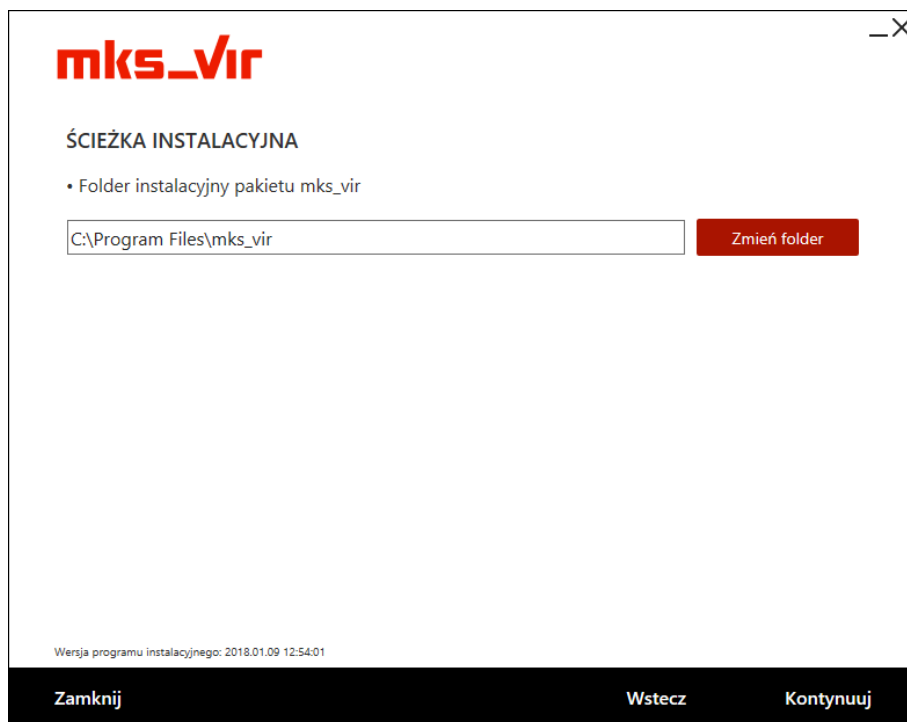
Po wybraniu „Kontynuuj”, zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku „Kontynuuj”:



pojawi się okno do wpisania numeru licencji:



Po wpisaniu numeru licencji i zatwierdzeniu przyciskiem „Kontynuuj” wybieramy folder instalacyjny **mks_vir** (sugerujemy pozostawienie domyślnego), po czym ponownie wciskamy przycisk „Kontynuuj”:



W kolejnym oknie wybieramy przycisk „Kontynuuj” bez wypełniania lub zmiany zawartości widocznych w nim pól:



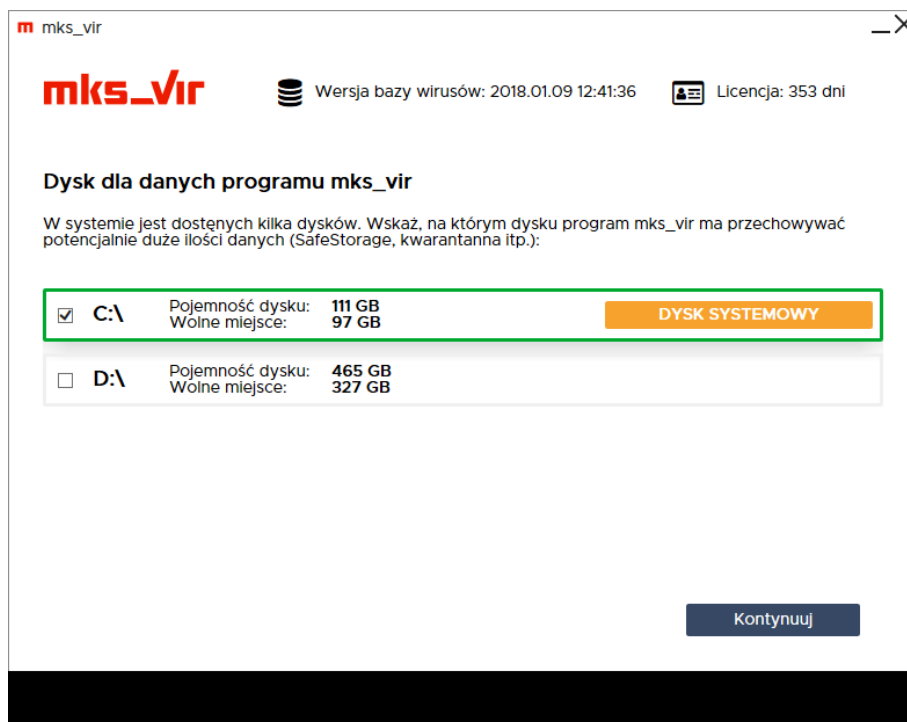
Rozpocznie się właściwa instalacja pakietu:



Poprawna instalacja programu zostanie zakończona oknem z informacją o pomyślnie przeprowadzonym procesie instalacji:



Jeśli w systemie jest dostępnych więcej dysków niż jeden, pojawi się okno z możliwością wyboru dysku dla folderu przechowywania dużej ilości danych programu **mks_vir**, takich jak kwarantanna, *SafeStorage* czy szyfrowane dyski (domyślnie sugerowany jest dysk z największą ilością wolnego miejsca):



Instalacja programu mks_vir administrator

Instalator **mks_vir administrator** przeznaczony jest do instalacji serwera zarządzającego **mks_vir administrator**

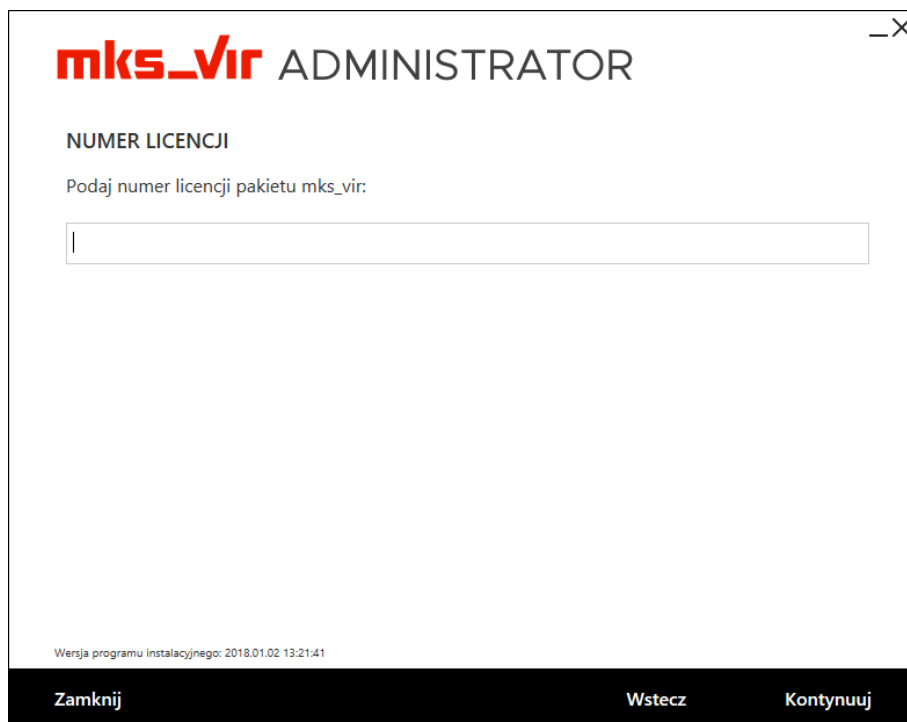
Po uruchomieniu instalatora pojawi się okno dialogowe umożliwiające rozpoczęcie instalacji programu:



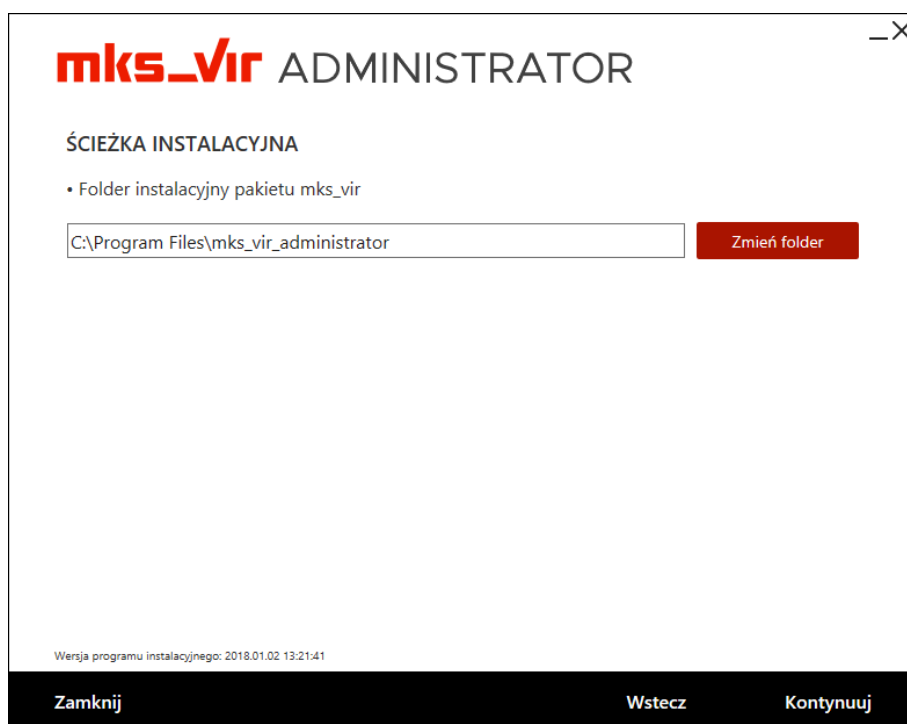
Po wybraniu „Kontynuuj”, zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku „Kontynuuj”:



pojawi się okno do wpisania numeru licencji:



Instalując **mks_vir administrator** najlepiej ścieżkę instalacyjną pozostawić domyślną:



a także domyślny „Numer portu” (Uwaga, program **mks_vir administrator** wykorzystuje cztery kolejne porty zaczynając od wpisanego w polu „Numer portu”, czyli domyślnie są to porty **4000, 4001, 4002 i 4003**). Konieczne jest także podanie hasła dostępowego dla administratora (admin) konsoli:



mks_vir ADMINISTRATOR

USTAWIENIA SERWERA

- Numer portu, który będzie wykorzystywany do komunikacji stacji z serwerem.

Uwaga: Do komunikacji będą wykorzystywane w sumie 4 kolejne porty począwszy od portu podanego.

Numer portu:

- Hasło użytkownika administracyjnego (admin) pakietu mks_vir administrator

Hasło:

Powtórz hasło:

Wersja programu instalacyjnego: 2018.01.02 13:21:41

Zamknij Wstecz Kontynuuj

Po wybraniu przycisku „Kontynuuj” rozpocznie się właściwa instalacja pakietu:



mks_vir ADMINISTRATOR

INSTALACJA



bin\mks_virupdate.exe

Wersja programu instalacyjnego: 2018.01.02 13:21:41

Poprawna instalacja programu zostanie zakończona oknem z informacją o pomyślnie przeprowadzonym procesie instalacji:



Instalacja programu mks_vir endpoint

Wersja **mks_vir endpoint** przeznaczona jest do instalacji jako stacja zarządzana przez **mks_vir administrator**

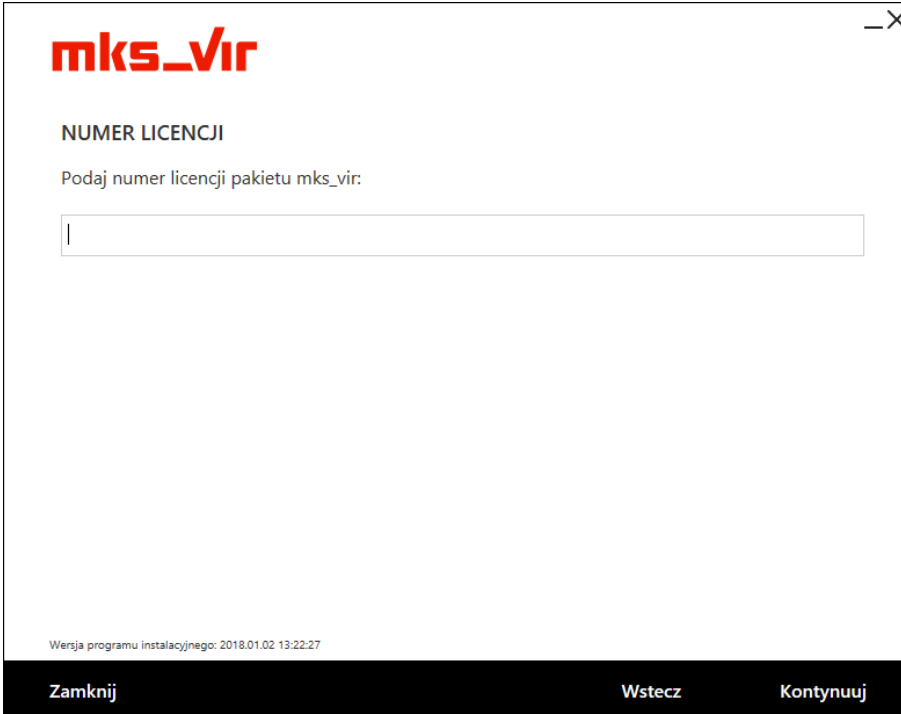
Po uruchomieniu instalatora pojawi się okno dialogowe umożliwiające rozpoczęcie instalacji programu:



Po wybraniu „Kontynuuj”, zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku „Kontynuuj”:

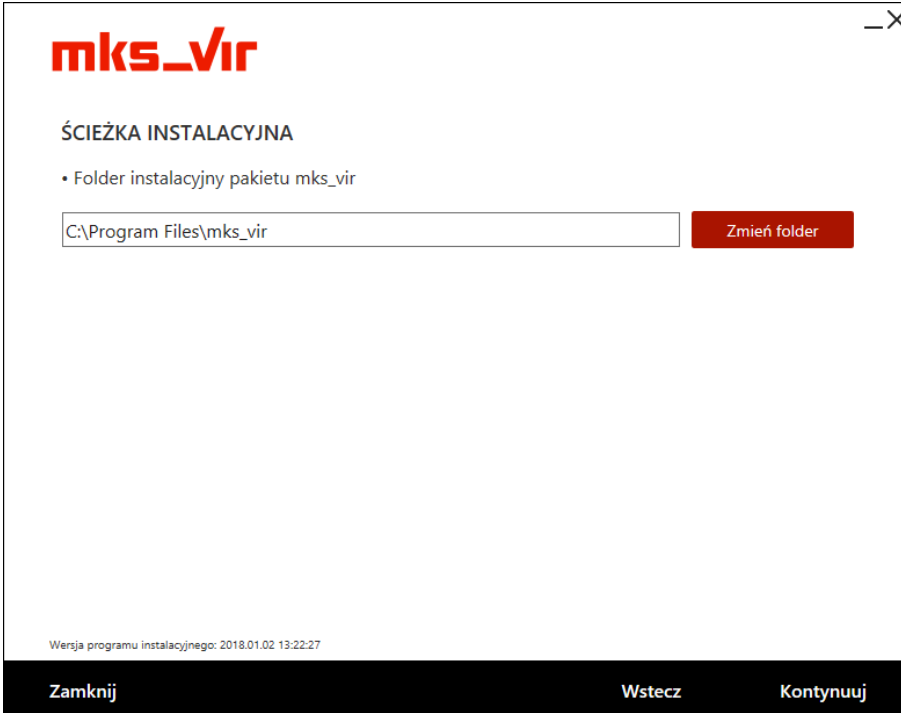


pojawi się okno do wpisania numeru licencji:



The screenshot shows a window titled "mks_vir" with a close button in the top right corner. The main heading is "NUMER LICENCJI". Below it, the text reads "Podaj numer licencji pakietu mks_vir:". There is a large empty text input field. At the bottom left, it says "Wersja programu instalacyjnego: 2018.01.02 13:22:27". The bottom bar contains three buttons: "Zamknij", "Wstecz", and "Kontynuuj".

Po wpisaniu numeru licencji i zatwierdzeniu przyciskiem „Kontynuuj” wybieramy folder instalacyjny **mks_vir** (sugerujemy pozostawienie domyślnego), po czym ponownie wciskamy przycisk „Kontynuuj”:



The screenshot shows a window titled "mks_vir" with a close button in the top right corner. The main heading is "ŚCIEŻKA INSTALACYJNA". Below it, there is a bullet point: "• Folder instalacyjny pakietu mks_vir". There is a text input field containing "C:\Program Files\mks_vir" and a red button labeled "Zmień folder". At the bottom left, it says "Wersja programu instalacyjnego: 2018.01.02 13:22:27". The bottom bar contains three buttons: "Zamknij", "Wstecz", and "Kontynuuj".

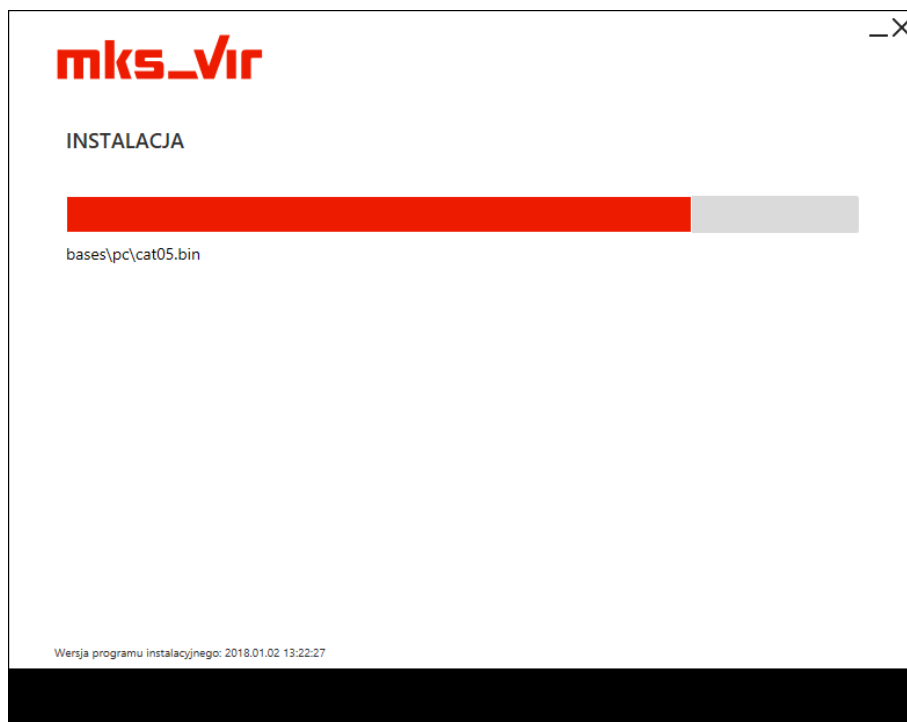
Następnie podajemy adres IP lub nazwę sieciową komputera, na którym został zainstalowany **mks_vir administrator**, czyli „Adres serwera”, sugerujemy by „Port” pozostawić domyślny (Uwaga, wpisany port musi być taki sam jak podany przy instalacji programu **mks_vir administrator**):



UWAGA! Podanie błędnego adresu IP lub jego brak spowoduje, że program nie będzie poprawnie współpracował z programem **mks_vir administrator**

Zaznaczona opcja „Sprawdź połączenie z serwerem przed kontynuacją instalacji” spowoduje, że program instalacyjny zweryfikuje poprawność adresu serwera zarządzającego (czyli czy serwer jest dostępny i aktywny pod podanym adresem) i dopiero w przypadku pozytywnej weryfikacji pozwoli na kontynuowanie instalacji.

Po wybraniu przycisku „Kontynuuj” rozpocznie się właściwa instalacja pakietu:



Poprawna instalacja programu zostanie zakończona oknem z informacją o pomyślnie przeprowadzonym procesie instalacji:



Automatyczna instalacja programu mks_vir

Automatyczna instalacja programu mks_vir w trybie niezarządzanym

Do automatycznej instalacji programu **mks_vir** w trybie niezarządzanym (*Internet Security*) należy zmodyfikować nazwę pliku instalacyjnego zgodnie z poniższym przykładem:

```
mks_virsetup2-serial(nr_licencji)auto(1).exe
```

gdzie:

- **serial(nr_licencji)** – umożliwia podanie numeru licencji koniecznego do instalacji programu **mks_vir**
- **auto(1)** – powoduje że proces instalacji przebiega całkowicie automatycznie, w przypadku braku opcji lub podanie „auto(0)” powoduje pojawianie się pytań tak, jak przy normalnej instalacji programu, przy czym odpowiednie pole będzie wypełnione zgodnie z parametrem „serial”

Automatyczna instalacja programu mks_vir w trybie zarządzanym

Do automatycznej instalacji programu **mks_vir** w trybie zarządzanym (*Endpoint Security*) należy zmodyfikować nazwę pliku instalacyjnego zgodnie z poniższym przykładem:

```
mks_virsetup2-serial(nr_licencji)server(adres_serwera)port(nr_portu)auto(1).exe
```

gdzie:

- **serial(nr_licencji)** – umożliwia podanie numeru licencji koniecznego do instalacji programu **mks_vir**
- **server(adres_serwera)** – umożliwia podanie adresu serwera administracyjnego **mks_vir administrator**, brak opcji instaluje program w trybie niezarządzanym
- **port(nr_portu)** – umożliwia zdefiniowanie portu komunikacyjnego **mks_vir administrator**, brak opcji przypisuje domyślny port „4000”
- **auto(1)** – powoduje że proces instalacji przebiega całkowicie automatycznie, w przypadku braku opcji lub podanie „auto(0)” powoduje pojawianie się pytań tak, jak przy normalnej instalacji programu, przy czym odpowiednie pola będą wypełnione zgodnie z parametrami „serial”, „server” i „port”

Automatyczna instalacja programu mks_vir w trybie zarządzanym w domenie Windows

Dane konieczne do instalacji programu **mks_vir** w trybie zarządzanym (*Endpoint Security*) w domenie Windows:

- **nr_licencji** – numer licencji konieczny do instalacji programu **mks_vir**
- **adres_serwera** – adres serwera administracyjnego **mks_vir administrator** (nie musi być to kontroler domeny)
- **nr_portu** – port komunikacyjny **mks_vir administrator** (domyślnym portem jest „4000”)
- **\\kontroler_domeny\zasob_mks_vir** – udostępniony do odczytu na kontrolerze domeny zasób, w którym należy umieścić skrypt instalacyjny *PowerShell* oraz plik instalatora **mks_virsetup2.exe**

Poniżej treść skryptu instalacyjnego *PowerShell*, w którym modyfikujemy zgodnie z posiadanymi danymi wartości zmiennych **\$serial**, **\$server**, **\$port** i **\$netpath** – reszta skryptu nie wymaga żadnych zmian:

```
Start-Sleep -Seconds 60
if(($(Get-Process mks_virsv) -eq $null) -or ($(Get-Process mks_virmon) -eq $null)) {
    $serial = 'nr_licencji'
    $server = 'adres_serwera'
    $port = 'nr_portu'
    $netpath = '\\kontroler_domeny\zasob_mks_vir'

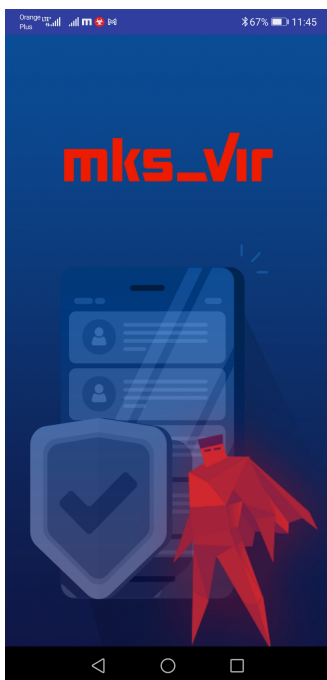
    $srcfile = $netpath + '\mks_virsetup2.exe'
    $dstfile = [System.Environment]::GetEnvironmentVariable('TEMP', 'Machine')
    $dstfile = $dstfile + '\mks_virsetup2-serial(' + $serial
    $dstfile = $dstfile + ')server(' + $server
    $dstfile = $dstfile + ')port(' + $port + ')auto(1).exe'

    Copy-Item $srcfile -Destination $dstfile
    Start-Process -Wait -FilePath $dstfile -Verb RunAs
    Remove-Item $dstfile
}
```

Wywołanie skryptu instalacyjnego należy umieścić w domenowym mechanizmie *GPO*, by był uruchamiany z uprawnieniami administratora domeny po starcie systemu na stacjach podłączonych do tej domeny. Skrypt sam sprawdzi, czy program **mks_vir** jest już zainstalowany na stacji i jeśli nie, rozpocznie jego instalację. Pozwala także na automatyczną naprawę programu w przypadku, gdy ten z jakiś przyczyn nie działa prawidłowo na stacji.

mks_vir dla systemu Android

Po uruchomieniu programu **mks_vir** dla systemu Android pojawia się plansza tytułowa programu:



a następnie ekran główny programu:



gdzie są wyświetlane podstawowe informacje na temat stanu programu, wersji baz wirusów oraz data ostatniego skanowania. Poza tym są do wyboru:

- **Skanowanie** – uruchamia skanowanie systemu pod kątem ew. obecności zagrożeń
- **Aktualizacja** – uruchamia aktualizację baz wirusów programu **mks_vir**; niezależnie od tej opcji program aktualizuje się automatycznie
- **Ustawienia** – otwiera okno umożliwiające indywidualną konfigurację programu **mks_vir**
- **Raporty** – umożliwia przejrzanie raportów z działania programu **mks_vir**

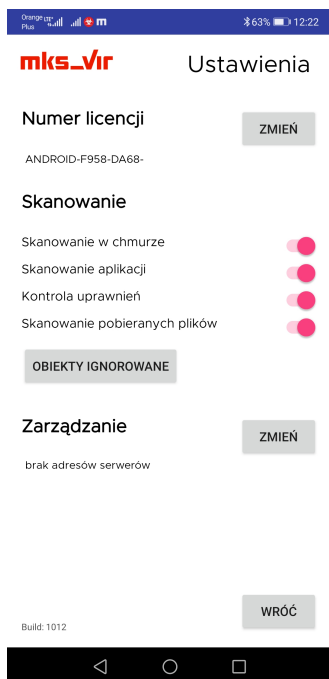
Po wybraniu **Skanowania** pojawia się okno wyświetlające progres skanowania systemu:



Po wybraniu **Aktualizacji** pojawia się okno wyświetlające status aktualizacji programu **mks_vir**:

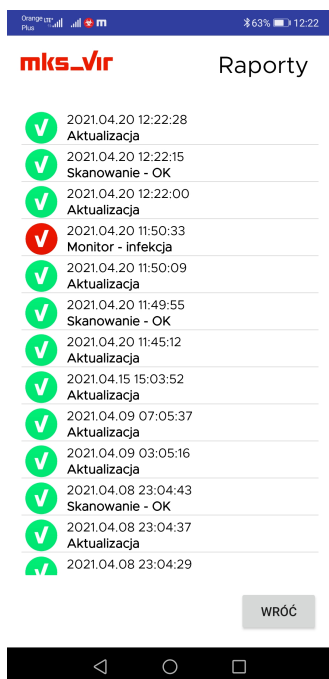


Po wybraniu **Ustawień** pojawia się okno umożliwiające indywidualne dostosowanie programu **mks_vir**:

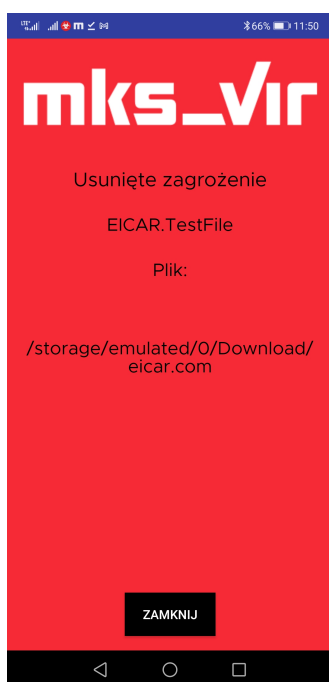


- **Numer licencji** – wyświetla początkowy fragment licencji, na której aktualnie działa program **mks_vir**; możliwa jest także zmiana tego numeru licencji za pomocą przycisku „Zmień”
- **Skanowanie** – pozwala na dostosowanie opcji skanowania i ochrony w programie **mks_vir**:
 - **Skanowanie w chmurze** – włącza wykorzystanie w czasie skanowania i ochrony systemu *chmurę obliczeniową mks_vir* – do poprawnego działania tej opcji jest konieczny dostęp do internetu
 - **Skanowanie aplikacji** – włącza skanowanie zainstalowanych w systemie Android aplikacji
 - **Kontrola uprawnień** – włącza weryfikację uprawnień aplikacji, co umożliwia ostrzeganie, gdy jakieś aplikacje mają zbyt wysoki poziom uprawnień
 - **Skanowanie pobieranych plików** – włącza automatyczne sprawdzanie pobieranych z internetu plików
- **Zarządzanie** – umożliwia podłączenie programu do konsoli administracyjnej **mks_vir administrator**; adres podajemy w formacie **adres:port**, gdzie:
 - **adres** – adres serwera zarządzającego **mks_vir administrator**
 - **port** – port komunikacyjny dla serwera zarządzającego **mks_vir administrator** (domyślnie 4000)

Po wybraniu **Raportów** pojawia się okno umożliwiające przejrzanie raportów aktywności programu **mks_vir**:



W przypadku znalezienia i usunięcia zagrożenia przez program **mks_vir** wyświetlane jest odpowiednie okno informacyjne:



Wymagania systemowe programów mks_vir

Programy **mks_vir** są kompatybilne z następującymi systemami operacyjnymi:

- **MS Windows 11**
- **MS Windows 10**
- **MS Windows 8.1**
- **MS Windows 8**
- **MS Windows 7** z dodatkiem *Service Pack 1* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows Vista** z dodatkiem *Service Pack 2* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows XP** z dodatkiem *Service Pack 3* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows Server 2025**
- **MS Windows Server 2022**
- **MS Windows Server 2019**
- **MS Windows Server 2016**
- **MS Windows Server 2012 R2**
- **MS Windows Server 2012**
- **MS Windows Server 2008 R2** z dodatkiem *Service Pack 1* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows Server 2008** z dodatkiem *Service Pack 2* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows Server 2003 R2** z dodatkiem *Service Pack 2* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **MS Windows Server 2003** z dodatkiem *Service Pack 2* oraz wszystkimi dostępnymi aktualizacjami ważnymi i opcjonalnymi
- **Android 8.0** lub nowszy

Programy **mks_vir** w systemach Windows wymagają do pracy zainstalowanego .NET Framework 4.0 lub nowszego.

Serwer i konsola zdalnego zarządzania wymagają do pracy systemów Windows Server 2008 R2 albo Windows 7 (oba z dodatkiem Service Pack 1) lub nowszych.

Umowa licencyjna

Poniższa umowa przedstawia postanowienia prawne zawarte pomiędzy firmą Arcabit Sp. z o.o. zwaną dalej Producentem, a Nabywcą jako końcowym użytkownikiem. Firma Arcabit Sp. z o.o. jest producentem programu antywirusowego **mks_vir**, zwanego dalej Programem. Jest on chroniony przez prawo polskie (Ustawa o Prawie Autorskim i Prawach Pokrewnych Dz. U. Nr 24, poz. 83) oraz międzynarodowe postanowienia o ochronie własności intelektualnych i prawnych.

Producent nie sprzedaje Nabywcy Programu, a jedynie udziela mu prawa jego użytkowania zgodnie z postanowieniami niniejszej Umowy. Producent zastrzega sobie wszelkie prawa nie wyrażone bezpośrednio w Umowie. Przyjmuje się, że Nabywca instalując program, akceptuje postanowienia tej umowy. Jeśli Nabywca nie akceptuje warunków umowy w ciągu 30 dni może zwrócić oprogramowanie w miejscu, gdzie zostało ono nabyte w zamian za zwrot zapłaconej kwoty w pełnej wysokości. Po upływie okresu aktualizacji Nabywca ma prawo do wykorzystywania Programu bez prawa do aktualizacji.

Producent zastrzega sobie prawo dołączenia do aktualizacji Programu materiałów informacyjno reklamowych o współpracujących z nim podmiotach trzecich oraz przesyłania informacji o produktach i promocjach producenta.

Nabywca ma prawo:

1. do użytkowania Programu na liczbie stanowisk określonych w licencji;
2. do pobierania aktualnej wersji Programu z Internetu przez czas określony w licencji, pod warunkiem dokonania instalacji nie później niż miesiąc od daty zakupu;
3. do uzyskania porad w przypadku trudności. Porad udzielają wysokiej klasy specjaliści;
4. do przesłania plików podejrzanych o infekcję nieznanym wirusem do analizy;
5. do uzyskania bezpłatnej szczepionki na dostarczonego wirusa, nieusuwalnego przez najnowszą wersję programu;
6. do bezpłatnego wsparcia technicznego przez okres trwania abonamentu;

Nabywca nie ma prawa:

1. do wypożyczania, wynajmowania lub innych form przekazywania udzielonej mu Licencji bez wcześniejszej pisemnej zgody Producenta;
2. wykonywania kopii programu, z wyjątkiem jednej kopii do celów archiwalnych;
3. modyfikowania, tłumaczenia, rekompilowania Programu oraz towarzyszącej mu dokumentacji w jakiegokolwiek postaci;
4. dokonywania prób odtwarzania kodu źródłowego Programu;
5. tworzenia produktów pochodnych na podstawie Programu;

6. usuwania lub zmiany znaków handlowych i informacji o produkcie podanych w Programie bądź w dołączonych materiałach;
7. świadczenia usług przy wykorzystaniu Programu;

Gromadzenie informacji

Oprogramowanie może przysyłać na serwery prowadzone przez Producenta informacje o plikach, o ich zawartości jak i ścieżce dostępu, a także fragmenty lub całe pliki, w celu ich weryfikacji pod kątem zagrożeń.

Uzyskane informacje są chronione przez Producenta zgodnie z wymogami ustawowymi.

Ograniczenia rękojmi

Producent gwarantuje, że Program będzie w znacznym stopniu działał zgodnie z dołączoną dokumentacją. Producent nie gwarantuje, że Program spełni oczekiwania nabywcy. Program jest intensywnie testowany w zakresie prawidłowości działania oraz współdziałania z różnorodnym oprogramowaniem, tym niemniej Producent nie gwarantuje całkowitej bezbłędności Programu oraz poprawnego współdziałania z innym oprogramowaniem. Producent nie ponosi odpowiedzialności za szkody wynikłe z użytkowania Programu lub braku możliwości użytkowania Programu niezależnie od tego w jaki sposób te szkody powstały i czego dotyczą. Nabywca ponosi pełne ryzyko co do możliwości użycia zakupionego Programu do określonego celu. W przypadku udostępnienia numeru licencji osobom trzecim Producent zastrzega sobie możliwość zablokowania numeru licencji bez wcześniejszego powiadomienia Nabywcy.

Wyłączenia z odpowiedzialności za straty

Producent nie ponosi odpowiedzialności za jakiegokolwiek przypadkowe, nieprzypadkowe, pośrednie lub podobne uszkodzenia, włącznie z każdą utratą korzyści lub danych, jakie powstały w wyniku użycia Programu nawet jeśli Producent został uprzedzony o możliwości powstania takich uszkodzeń. Zrzeczenia i ograniczenia wymienione powyżej będą miały zastosowanie niezależnie od tego, czy nabywca zaakceptuje Program. W żadnym z przypadków odpowiedzialność Producenta względem Nabywcy na podstawie postanowień niniejszej umowy nie przekroczy sumy, jaką Nabywca uiszczył za licencję na korzystanie z programu.