



mks_vir 2
• Skanowanie
• Ochrona
• Aktualizacja
• Licencja
• Ustawienia
• Raporty
• Narzędzia
• Informacje
Szczegółowe ustawienia pakietu
Ochrona $ ightarrow$ Ochrona plików
Ochrona $\rightarrow$ SafeStorage
Ochrona $ ightarrow$ Ochrona poczty
Ochrona $ ightarrow$ Ochrona przeglądarki $\ldots$
Ochrona $ ightarrow$ Zapora sieciowa (firewall) $\ \ \ldots $
Ochrona $ ightarrow$ Kontrola urządzeń USB $\ldots$
Ochrona $ ightarrow$ Kontrola urządzeń multimedialnych
Ochrona $ ightarrow$ Kontrola aplikacji $\ldots$
Ochrona $\rightarrow$ Ochrona RoundKick EDR $\dots \dots 22$
Ochrona $ ightarrow$ Bezpieczna przeglądarka $\ldots$
Skanowanie $\rightarrow$ Skanowanie pełne
Skanowanie $\rightarrow$ Skanowanie szybkie
Skanowanie $\rightarrow$ Kwarantanna
Kontrola rodzicielska
Aktualizacja
Ogólne
Aktualizacja programu w sieciach lokalnych za pomocą mechanizmu repozytorium udostępnianego po HTTP
Aktualizacja programu na stacjach bez dostępu do sieci za pomocą mechanizmu repozytorium
Sygnalizacja wykrycia zagrożenia przez moduł "Ochrona plików" 40
Sygnalizacja próby połączenia przez moduł "Zapory"

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	117
Podstawowe informacje o grupie	117
	120
	124
	125
• Oprogramowanie	128
Podsumowanie	128
	130
$Ochrona \rightarrow Ochrona pilkow \dots \dots$	130
$Ochrona \rightarrow SateStorage \dots \dots$	131
Ochrona $\rightarrow$ Ochrona poczty	123
Ochrona $\rightarrow$ Ochrona przeglądarki	134 105
Ochrona $\rightarrow$ Zapora sieciowa (firewali)	135
()chrona → Kontrola urządzeń LISB	136

Ochrona $ ightarrow$ Kontrola urządzeń multimedialnych	138
$Ochrona \to Kontrola \; aplikacji \; \ldots \; $	139
$Ochrona \to Ochrona \ RoundKick \ EDR \ \ \ldots $	140
$Ochrona \to Bezpieczna \ przegl{}_{q}darka  . \ . \ . \ . \ . \ . \ . \ . \ . \ .$	142
Skanowanie $ ightarrow$ Skanowanie pełne $\ \ldots \ $	143
Skanowanie $ ightarrow$ Skanowanie szybkie $\ \ldots \ $	144
Skanowanie $\rightarrow$ 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 zachowa- niem 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:



#### 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:

Image: Add to the type of the type of the type of the type of type	n mks_vir		0_×
Ochrona         Xtywność poszczególnych modułów ochronnych         Image: Chrona pilków	mks_VI	Wersja bazy wirusów: 2022.11.29 07:58:40	Licencja: 764 dni
Aktywność poszczególnych modułów ochronnych       Tymczasowo wyłącz ochroną         Image: Controna plików       Image: Controna plików         Image: Controna poczty       Image: Controna poczty         Image: Controna przeglądarki       Image: Controna przeglądarki         Image: Controna rodzicielska       Image: Controna rodzicielska         Image: Controna urządzeń multimedialnych       Image: Controna regestru         Image: Controna regestru       Image: Controna regestru         Image: Controna w chmurze       Image: Controna RoundKlick EDR	Ochrona		
<ul> <li>Ochrona plików</li> <li>Ochrona poczty</li> <li>Ochrona przeglądarki</li> <li>Zapora sieciowa (firewall)</li> <li>Kontrola rodzicielska</li> <li>Kontrola urządzeń USB</li> <li>Kontrola urządzeń multimedialnych</li> <li>Kontrola aplikacji</li> <li>Ochrona rejestru</li> <li>Ochrona rejestru</li> <li>Ochrona w chmurze</li> <li>Ochrona RoundKick EDR</li> </ul>	Aktywność poszcze	ególnych modułów ochronnych	Tymczasowo wyłącz ochronę
Ochrona pocztyCSochrona przeglądarkiCSochrona przeglądarkiCSapora sieciowa (firewall)CKontrola rodzicielskaCSochrona urządzeń USBCKontrola urządzeń multimedialnychCKontrola aplikacjiCOchrona rejestruCOchrona w chmurzeCOchrona RoundKick EDRC	U	Ochrona plików	
<ul> <li>Ochrona przeglądarki</li> <li>Zapora sieciowa (firewall)</li> <li>Kontrola rodzicielska</li> <li>Kontrola urządzeń USB</li> <li>Kontrola urządzeń multimedialnych</li> <li>Kontrola aplikacji</li> <li>Ochrona rejestru</li> <li>Ochrona w chmurze</li> <li>Ochrona RoundKick EDR</li> </ul>		Ochrona poczty	
<ul> <li>Zapora sieciowa (firewall)</li> <li>Kontrola rodzicielska</li> <li>Kontrola urządzeń USB</li> <li>Kontrola urządzeń multimedialnych</li> <li>Kontrola aplikacji</li> <li>Ochrona rejestru</li> <li>Ochrona w chmurze</li> <li>Ochrona RoundKick EDR</li> </ul>	<del>o</del> o	Ochrona przeglądarki	
Kontrola rodzicielska)Kontrola urządzeń USB)Kontrola urządzeń multimedialnych)Kontrola aplikacji)Kontrola aplikacji)Cochrona rejestru)Ochrona w chmurze)Ochrona RoundKick EDR)	A	Zapora sieciowa (firewall)	
Kontrola urządzeń USB       )         Kontrola urządzeń multimedialnych       )         Kontrola aplikacji       )         Ochrona rejestru       )         Ochrona w chmurze       )         Ochrona RoundKick EDR       )	Ť	Kontrola rodzicielska	$\bigcirc$
Kontrola urządzeń multimedialnychKontrola aplikacjiKontrola aplikacjiOchrona rejestruOchrona w chmurzeOchrona RoundKick EDR	● <del>∕`</del> ∎	Kontrola urządzeń USB	$\bigcirc$
Kontrola aplikacji       Image: Constrution of the sector of	Ō	Kontrola urządzeń multimedialnych	$\bigcirc$
Ochrona rejestru     Image: Construit of the second s	00	Kontrola aplikacji	$\bigcirc$
Ochrona w chmurze     Ochrona RoundKick EDR	&	Ochrona rejestru	
Ochrona RoundKick EDR	8	Ochrona w chmurze	
	4	Ochrona RoundKick EDR	

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):

i yiliczasowe wyłąc.	terile ochrony mks_v	41		
Ta funkcja pozwala n Po wskazanym poniż	a czasowe wyłączenie w ej czasie ochrona został	wszystkich modułów nie automatycznie w	/ ochronnych pakietu mks_v /znowiona.	/ir.
Wybierz, przez jaki okr	es ochrona mks_vir ma	być wyłączona:		
IO minut				
🔾 20 minut				
0 30 minut				
O Do ponownego uru	nomienia systemu			
Wyłącz ochronę				
			Zan	nknii

## 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:**

m mks_vir		0 _×
mks_Vr s	Wersja bazy wirusów: 2025.03.17 08:54:20	Licencja: 655 dni
Raporty	Raj	oorty z dnia: 2025-03-17
Data	Zdarzenie	Status
2025-03-17 10:07:31	Aktualizacia pakietu	~
2025-03-17 07:42:05	Aktualizacja pakietu	<ul> <li>Image: A set of the set of the</li></ul>
2025-03-17 04:41:49	Aktualizacja pakietu	✓
2025-03-17 01:41:19	Aktualizacja pakietu	✓
Pokaż tylko raporty o Infekcjach		Pokaż aktywność sieciową
A C	X 🛡 📩 🖅 🌣 💆 🎤	<b>i</b>

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	Raporty o	) infekcjach z ostatnich 30 dr
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

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

mks_vir - aktywność sieciowa							-		×
Aktywność sieciowa z dnia	: 2025.04.17	,		Dane lokalizacyjne	dostar	cza ᠙ IP	info		
Filtry		···	:						
	07:49:35	msedge.exe	7	212.77.98.33	443			Poland	~
	07:49:04	tasknostw.exe	~	104.208.16.94	443			United	ST
	07:49:03	msedge.exe	7	142.250.203.138	443			Poland	
🗹 Przychodzące < 🛛	07:49:03	msedge.exe	<b>→</b>	212.77.106.3	443			Poland	
Wychodzace - 303	07:48:29	svchost.exe	→	199.232.214.172	80			United	St
	07:48:24	msedge.exe	<b>&gt;</b>	150.171.28.11	443			United	St
🗸 IP v4 303	07:48:24	msedge.exe	→	150.171.27.11	443			United	St
VIP v6 0	07:48:24	msedge.exe	<b>&gt;</b>	2.20.33.159	443	-		Poland	
Aplikacie	07:48:24	msedge.exe	→	13.107.253.44	443			United	St
	07:48:24	msedge.exe	<b>&gt;</b>	13.107.246.44	443			United	St
Mousocoreworker.exe	07:48:24	msedge.exe	<b>&gt;</b>	13.107.253.44	443			United	St
msedge.exe	07:48:12	msedge.exe	÷	35.210.199.153	443			Belgiu	m
msedgewebview2.exe	07:48:09	msedge.exe	÷	212.77.98.63	443	-		Poland	
✓ msmpeng.exe	07:48:08	msedge.exe	÷	212.77.98.63	443			Poland	
< searchapp.exe	07:48:08	msedge.exe	÷	212.77.98.63	443			Poland	
✓ smartscreen.exe	07:48:08	msedge.exe	÷	212.77.98.63	443	-		Poland	
✓ svchost.exe	07:48:08	msedge.exe	÷	212.77.98.63	443			Poland	
vstemsettings.exe	07:48:08	msedge.exe	÷	142.250.186.194	443	-		Poland	
taskhostwexe	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 ( $\leftarrow$ ) lub wychodzących ( $\rightarrow$ )

- dla połączeń na protokołach IP v4 lub IP v6
- Aplikacje pozwala na filtrację aktywności połączeń dla określonych aplikacji

#### Narzędzia:

m mks	_vir				(	9_×
П	ıks_Vır	🛢 Wersja b	azy wirusów: 2025.(	06.24 10:34:54	Licencja: 556 dni	
Na	rzędzia					
	<b>†</b>	盦		ආ		
	Kwarantanna	SafeStorage	Bezpieczna przeglądarka	Kopie zapasowe	Menadżer procesów	
	<u>hh</u>		6		<b>&amp;</b>	
	Audyt systemu	Rescue Disk	Czyszczenie systemu	Windows Update	Wsparcie online	
	Q.	*		.th	~	
	Szyfrowane dyski	Menadżer haseł	Zarządzanie pakietem	Konsola administracyjna	Stan systemu	
	1			v 🦊 i		

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:
  - m mks\_vir stan systemu × TEST101 <del>C.</del> Ø Wydajność systemu (procesor/pamięć/starty systemu) ostatnia godzina ostatnie 24 godziny ostatnie 7 dni ostatnie 30 dni Procesor 7% 100% 0% Pamięć 49% 100% 0% () Starty systemu 1

Wydajność systemu:

– Dyski:

	Ø					Ţ	TES
ski							
sta dysk	ów fizycznych						
Model		Serial	Rozmiar	Partycje			
ST1000	DM010-2EP102	Z9AP4S4Z	931.5 GB	Z:			
ADATA	SU800	2H4320092706	119.2 GB	C:			
atus dy:	sków fizycznych	(S.M.A.R.T.)		C			
atus dy: 📀 Status	sków fizycznych ADATA SU8 Parameter	(S.M.A.R.T.)	Curre	C: ent Worst	Threshold	Data	
atus dys Status	sków fizycznych ADATA SU8 Parameter Raw read erro	(S.M.A.R.T.) 000	Curre 100	C: ent Worst 100	Threshold 0	Data 0	
atus dy: Status	sków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se	(S.M.A.R.T.) 000 or rate (1) ector count (5)	Curre 100 100	C: ent Worst 100 100	Threshold O O	Data O 1	
atus dy: Status A	sków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou	(S.M.A.R.T.) 000 or rate (1) ector count (5) irs count (9)	Curre 100 100 100	C: ent Worst 100 100 100	Threshold O O O	Data 0 1 3837	
atus dy: Status A O	sków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle c	(S.M.A.R.T.) 000 or rate (1) ector count (5) irs count (9) ount (12)	Curre 100 100 100 100	C: 100 100 100 100	Threshold O O O O	Data 0 1 3837 1795	
atus dy: Status O A O O O	sków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle c Power-off retr	(S.M.A.R.T.) 000 or rate (1) ector count (5) irs count (9) ount (12) ract count (192)	Curre 100 100 100 100 100	C: 100 100 100 100 100 100	Threshold O O O O O O	Data O 1 3837 1795 48	
atus dy: Status A O O O	sków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle c Power-off retr HDD temperal	(S.M.A.R.T.) 200 201 201 201 201 201 201 201	Curre 100 100 100 100 100 100	C: 100 100 100 100 100 100 100	Threshold           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0	Data 0 1 3837 1795 48 40	

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



– Przeglądarki:

Przeglądarki Strony z ustawieniam Wszystkie Dozwo C Edge Strona https://tvn24.pl:443,* https://www.gazeta.p	ni powiadomień olone Zabloł	(2025.06.24 Rowane Dc	4 10:36:3 omyślne
Przeglądarki Strony z ustawieniam Wszystkie Dozwo C Edge Strona https://tvn24.pl:443,* https://www.gazeta.p	ni powiadomień olone Zabloł	(2025.06.24 cowane Do	4 10:36:3 omyślne
Strony z ustawieniam Wszystkie Dozwo C Edge Strona https://tvn24.pi:443,* https://www.gazeta.p	ni powiadomień rolone Zabioł	(2025.06.24	4 10:36:3
Wszystkie Dozwo C Edge Strona https://tvn24.pi.443,* https://www.gazeta.p	rolone Zabloł	xowane Do	omyślne
Edge Strona https://tvn24.pl:443,* https://www.gazeta.p			mysine
Edge Strona https://tvn24.pl:443,* https://www.gazeta.p			
Edge Strona https://tvn24.pl:443,* https://www.gazeta.p			
Strona https://tvn24.pl:443,* https://www.gazeta.p			
https://tvn24.pl:443,* https://www.gazeta.p	Profil	Użytkownik	Status
https://www.gazeta.p	• Default	tester	Allow
	pl:443,* Default	tester	Deny
https://www.interia.pl	ol:443,* Default	tester	Deny
https://www.onet.pl:4	443,* Default	tester	Allow
https://www.wp.pl:44	43,* Default	tester	Deny

# Informacje:

Sprzęt i system Procesor:	Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz (3600 MHz)
Srafika:	Intel(R) UHD Graphics 630
Dvski:	C: 118.5 GB 85.7 GB Z: 447 GB 405.6 GB
System:	Microsoft Windows 11 Pro (64-bitowy)
Pakiet mks_vir	
lumer licencji:	TESTY-789B-BA94
icencja:	764 dni
Versja bazy:	2022.11.29 07:58:40
Kontakt	
n <b>ks_vir Sp. z o.</b> II. Graniczna 50 )5-082 Blizne Ła Warszawa/Bem piuro@mks-vir.pl Ittp://www.mks-	o. iszczyńskiego owo) <u>-vir.pl</u>

Informacje na temat systemu, stanu licencji i aktualizacji programu **mks\_vir** oraz informacje kontaktowe.

# Szczegółowe ustawienia pakietu

## $\textbf{Ochrona} \rightarrow \textbf{Ochrona} \text{ plików:}$



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 umożliwia 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 nosiciele** opcja powoduje, że sprawdzane są tylko pliki będące domyślnymi nosicielami zagrożeń, jak np. pliki EXE, COM, JS, VBS itp.
- Blokuj autostart na nośnikach USB uniemożliwia automatyczne uruchomienie z podłączanych pendrive potencjalnych zagrożeń
- **Optymalizuj dostęp do zasobów chmurowych** optymalizuje skanowania obiektów przechowywanych w chmurze (np. Microsoft Onedrive, Google Drive itp.)
- **Optymalizuj dostęp do przeglądarek internetowych** optymalizuje wydajność pracy przeglądarek internetowych (np. Microsoft Edge, Google Chrome itp.)

### $\textbf{Ochrona} \rightarrow \textbf{SafeStorage:}$

*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.





**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

#### $\textbf{Ochrona} \rightarrow \textbf{Ochrona poczty:}$



**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:

m mks vir 📀	$ \ge \times $
Zaawansowane ustawienia skanowania poczty	
Poczta przychodząca	
<ul> <li>✓ Skanuj pocztę przychodzącą</li> <li>✓ Załączniki wykonywalne traktuj jak zagrożenie</li> <li>✓ Skrypty w załącznikach traktuj jak zagrożenie</li> </ul>	ł
Poczta wychodząca	- 8
☑ Skanuj pocztę wychodzącą ☑ Dodaj stopkę do wysyłanych wiadomości	
	ł
	ł
	ł
	ł
Zamknij	I I

**Poziom heurystyki** – określa poziom pracy modułów heurystycznych; im wyższy poziom, tym większa skuteczność, ale także większa możliwość wystąpienia tzw. "fałszywych alarmów" **Akcje** – umożliwia wybranie automatycznej akcji, która ma być wykonana w przypadku znalezienia zagrożenia przez moduł ochrony poczty; do wyboru są następujące możliwości:

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

Antyspam – moduł do znakowania wiadomości-śmieci

#### $\textbf{Ochrona} \rightarrow \textbf{Ochrona} \text{ przeglądarki:}$

m mks_vir	0_×
mks_Vır	Se Wersja bazy wirusów: 2023.06.23 07:06:56 🛛 🖅 Licencja: 559 dni
ochrona	V 🏛 🖂 💁 🛦 🏎 🖸 端 1 🚍
<b>Q</b> skanowanie	✓ Aktywuj ochronę przeglądarki Poziom heurystyki
kontrola rodzicielska	Normalny  Ustawienia blokowania
🛃 aktualizacja	☑ Blokuj pobieranie niepodpisanych plików wykonywalnych □ Blokuj transmisje strumieniowe (audio/video) □ Blokuj popularne serwisy reklamowe
ogólne	Ustawienia dodatkowe
	□ Włącz rozszerzone skanowanie http/https
	🖀 Q 🛡 🚣 📧 🌞 💆 🗲 🚯

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

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

#### Ustawienia blokowania

- Blokuj pobieranie niepodpisanych plików wykonywalnych włączenie tej opcji powoduje, że przy próbie pobrania niepodpisanych cyfrowo plików wykonywalnych (czyli takich, dla których nie da się automatycznie zweryfikować poprawności pochodzenia pliku), zostanie wyświetlone odpowiednie ostrzeżenie; użytkownik będzie mógł wtedy podjąć decyzję, czy dany plik pobrać, czy jednak nie
- Blokuj transmisje strumieniowe (audio/video) włączenie tej opcji powoduje blokowanie wszelkiego rodzaju transmisji strumieniowych (co na przykład uniemożliwia słuchanie stacji radiowych przez internet)

 Blokuj popularne serwisy reklamowe – włączenie tej opcji powoduje blokowanie wyświetlania różnego rodzaju reklam pochodzących z najpopularniejszych serwisów reklamowych (włączenie opcji *Włącz rozszerzone skanowanie http/https* rozszerza zakres blokowanych reklam)

#### Ustawienia dodatkowe

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

#### $\textbf{Ochrona} \rightarrow \textbf{Zapora sieciowa (firewall):}$

<ul> <li>Wersja bazy wirusów: 2023.06.23 07:06:56</li> <li>Leencja: 559 dnl</li> <li>ochrona</li> <li>ochron</li></ul>
ochrona   Q   skanowanle
Q       skanowanie         ✓       Aktywuj zaporę sieciową         ✓       Dostosuj aktywność zapory Windows do zapory mks_vir         ✓       Przepuszczaj połączenia wychodzące         ✓       Przepuszczaj połączenia w sieci lokalnej         Włącz tryb cichy       ✓         ✓       Blokuj aktywność sieciową skryptów         Blokuj połączenia IPv6          ✓       Reguły zapory sieciowej
Ogólne         Definicje sieci lokalnych           Podaj definicje sieci lokalnych oddzielając je spacjami, np.: 192.168.0.0/16 172.16.0.0/12 10.0.0/8 FE80::/10 FC00::/7           192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 169.254.0.0/16 FE80:

Aktywuj zaporę sieciową – aktywuje moduł ochrony sieci

- Dostosuj aktywność zapory Windows do zapory mks\_vir aktywność tej opcji umożliwia automatyczne przełączanie aktywności zapory Windows w zależności od aktywności zapory mks\_vir; aktwacja zapory mks\_vir wyłącza zaporę Windows, zaś dezaktywacja zapory mks\_vir włącza zaporę Windows, dzięki czemu w systemie stale jest aktywna zapora
- Przepuszczaj połączenia wychodzące dopuszcza wszystkie połączenia wychodzące; większość połączeń sieciowych, to połączenia wychodzące (np. typowa aktywność przeglądarki w czasie surfowania po internecie) i takie połączenia są w ogromnej większości bezpieczne
- Przepuszczaj połączenia w sieci lokalnej aktywność tej opcji powoduje, że wszelkie połączenia nawiązywane w sieci lokalnej (połączenia wychodzące i przychodzące) są przepuszczane

- 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

## $\textbf{Ochrona} \rightarrow \textbf{Kontrola} \text{ urządzeń USB:}$



Aktywuj kontrolę urządzeń USB – aktywuje moduł kontroli urządzeń USB

Ustawienia – umożliwia konfigurację modułu kontroli urządzeń USB

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

- Blokuj blokuje każde nowe podłączane urządzenie USB
- Dopuść dopuszcza każde nowe podłączane urządzenie USB
- 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 "Dopuść" (przy podłączaniu nowych urządzeń USB)

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

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

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

Urządze	enie	Dostęp	
 _			

### $\textbf{Ochrona} \rightarrow \textbf{Kontrola} \ \textbf{urządzeń} \ \textbf{multimedialnych:}$



**Aktywuj kontrolę urządzeń multimedialnych** – aktywuje moduł kontroli urządzeń multimedialnych

Ustawienia – umożliwia konfigurację modułu kontroli urządzeń multimedialnych

- Gdy brak reguły umożliwia wybranie akcji, która ma być wykonana w przypadku próby dostępu do urządzenia multimedialnego przez aplikację, dla której nie jest zdefiniowana odpowiednia reguła (dopuszczająca lub blokująca); do wyboru są następujące możliwości:
  - Blokuj blokuje próbę dostępu do urządzenia multimedialnego przez aplikację
  - Dopuść dopuszcza próbę dostępu do urządzenia multimedialnego przez aplikację
  - 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 blokujacych lub dopuszczajacych dostęp do urządzeń multimedialnych przez aplikacje

 Dopuszczaj standardowe serwisy multimedialne Windows – zezwala na dostęp do urządzeń multimedialnych systemowym serwisom obsługi takich urządzeń bez konieczności tworzenia odpowiednich reguł **Pokaż listę reguł dla urządzeń multimedialnych** – umożliwia definiowanie lub modyfikację własnych reguł blokujących lub dopuszczających dostęp do urządzeń multimedialnych przez aplikacje:

m mks vir	<u> </u>
Lista reguł dla urządzeń multimedialnych	
	_
A = 10	Destar
Аріїкасја	Dostęp
Daniel as mult	Zenetreli
Dodaj reguię	Zamknij

#### $Ochrona \rightarrow Kontrola aplikacji:$



Aktywuj kontrolę aplikacji – aktywuje moduł kontroli aplikacji Ustawienia – umożliwia konfigurację modułu kontroli aplikacji  Włącz powiadomienia o zablokowaniu aplikacji – włącza wyświetlanie okien powiadomień modułu kontroli aplikacji w przypadku zablokowania próby uruchomienia aplikacji, dla której została zdefiniowana reguła blokująca

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

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

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

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

m mks vir Lista reguł dla aplikacji			0_)
Proces nadrzędny (uruchamiający)	Aplika	acja	Dostęp
Dodaj regułe			Zamknii

#### $\textbf{Ochrona} \rightarrow \textbf{Ochrona RoundKick EDR:}$

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 natychmia-stowa 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 skanująch 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)

#### $\textbf{Ochrona} \rightarrow \textbf{Bezpieczna} \ \textbf{przeglądarka:}$



- 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 $\rightarrow$ Skanowanie pełne:



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

- Usuń zagrożenia leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- Skasuj plik kasuje zainfekowane pliki
- Przenieś do kwarantanny przenosi zainfekowane pliki do folderu kwarantanny mks\_vir
- 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 $\rightarrow$ Skanowanie szybkie:



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

- przy starcie systemu
- po zalogowaniu użytkownika
- po aktualizacji programu mks\_vir
- po podłączeniu nośnika USB skanowana jest wtedy zawartość takiego nośnika

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

- Usuń zagrożenia leczy lub gdy tego nie da się wykonać (np. w przypadku trojanów), kasuje zainfekowane pliki
- Skasuj plik kasuje zainfekowane pliki
- Przenieś do kwarantanny przenosi zainfekowane pliki do folderu kwarantanny mks\_vir
- 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 $\rightarrow$ Kwarantanna:



Automatyczne skanowanie i czyszczenie ze starych plików kwarantanny programu mks\_vir:

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

### Kontrola rodzicielska:



**Aktywuj kontrolę rodzicielską** – uaktywnia moduł kontroli rodzicielskiej; 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 zdefiniowane własnych reguł przepuszczających lub blokujących w oparciu o adresy lub frazy (słowa kluczowe)

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

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

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

**Pokaż historię przeglądanych stron** – umożliwia przejrzenie 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 – umożliwia 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. tworzonego, aktualizowanego i udostępnianego przez program mks\_vir nie zarządzany z poziomu programu mks\_vir administrator)
- Zasób lokalny aktualizacje będą się odbywały z repozytorium dostępnego na lokalnym nośniku, np. na pendrive; opcja może mieć znaczenie dla sieci całkowicie odciętych od Internetu

#### Opcje aktualizacji:

Harmonogram aktualizacji – umożliwia określenie, kiedy ma być bezwzględnie wymuszana aktualizacja programu mks\_vir

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

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

**Repozytorium** – umożliwia 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:

m mks_vir	•_×		
mks_Vır	See Wersja bazy wirusów: 2023.04.13 08:11:55 Image Licencja: 629 dni Image Licencja: 629 dni		
<b>U</b> ochrona	Chroń hasłem ustawienia pakietu mks_vir     Ustawienia szczegółowe		
Skanowanie	Globalne wykluczenia ochrony		
$\sim$	Lista wykluczonych domen internetowych		
🔶 kontrola	Lista wykluczonych plików i folderów		
Lista wykluczonych procesów			
Aktualizacja Porty i protokoły			
Tabela skanowanych i wykluczonych portów i protokołów			
ogólne Folder danych			
Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zapasowe, szyfrowane dyski.			
🗹 Korzystaj z domyślnego folderu danych pakietu mks_vir			
	者 Q U 초 📧 🌻 🖾 ۶ 🕄		

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

m mks vir	0_
Ustawienia szczegółowe	
Aktywuj autoochronę pakietu mks_vir     Nie     Kopiuj leczone pliki do kwarantanny     Wy     Włącz kontrolę zajętości procesora     Wła     Aktywuj ochronę w chmurze     Poł     Aktywuj ochronę rejestru     Poł     Zezwalaj na protokół QUIC     Włącz akcelerację aktualizacji systemu Windows     Włącz akcelerację udostępniania szyfrowanych dy     Pokaż konsolę szyfrowanych dysków po zalogowa     Pokaż konsolę administracyjną w menu mks_vir w     Pokazuj ostrzeżenia o kończących się zasobach     Pokazuj ostrzeżenia o kończących się zasobach	skanuj połączeń lokalnych http krywaj aplikacje typu <i>Asystent pobierania</i> icz niskopoziomowe wykluczenia zapory aż grę Coolka w menu mks_vir w zasobniku aż klasyczną ikonę mks_vir w zasobniku sków niu zasobniku rnymi ch
Wyłacz komputer o godzinie:	amentu
Cablokuj system po czasie nieaktywności (w m	inutach):
	Zamknij

- Aktywuj autoochronę pakietu mks\_vir włącza mechanizmy chroniące spójność instalacji programu mks\_vir
- Kopiuj leczone pliki do kwarantanny tworzy w kwaranatannie programu mks\_vir kopie plików leczonych lub kasowanych; funkcja pomocna w przypadku, gdyby była konieczność przywrócenia orginalnych plików (sprzed leczenia) lub wysłania ich do ponownej analizy do działu analiz mks\_vir
- Włącz kontrolę zajętości procesora włącza mechanizm zmniejszający wykorzystanie mocy obliczeniowej procesora przez mechanizmy ochronne programu mks\_vir na mało wydajnych maszynach
- Aktywuj ochronę w chmurze włącza mechanizmy ochronne programu mks\_vir korzystające z możliwości chmury obliczeniowej mks\_vir; do działania wymagany jest stały dostęp do internetu
- Aktywuj ochronę rejestru włącza mechanizmy programu mks\_vir chroniące zawartość i spójność rejestru systemowego
- Zezwalaj na protokół QUIC wyłącza blokadę protokołu QUIC (HTTP/3):

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

- Nie skanuj połączeń lokalnych http wyłącza skanowanie protokołu HTTP dla połączeń realizowanych wewnątrz systemu operacyjnego (dla połączeń w adresacji 127.x.x.x)
- Wykrywaj aplikacje typu Asystent pobierania włącza wykrywanie tzw. Asystentów pobierania jako zagrożeń
- Pokaż konsolę szyfrowanych dysków po zalogowaniu włącza automatyczne wyświetlanie konsoli zarządzającej szyfrowanymi dyskami w programie mks\_vir po zalogowaniu użytkownika w systemie
- Włącz akcelerację udostępniania szyfrowanych dysków przyspiesza podłączanie szyfrowanych dysków do systemowych mechanizmów obsługi systemów plików
- Pokaż konsolę administracyjną w menu mks\_vir w zasobniku włącza dostęp do konsoli administracyjnej programu mks\_vir administrator w menu podręcznym ikony mks\_vir w zasobniku systemowym
- Włącz niskopoziomowe wykluczenia zapory włącza obsługę wykluczeń plików lub folderów zdefiniowanych w sekcji *Lista wykluczonych plików i folderów*, w zaporze programu mks\_vir
- Włącz akcelerację aktualizacji systemu Windows automatyzuje i przyspiesza instalację nowych aktualizacji systemu Windows
- Pokazuj ostrzeżenia o problemach z dyskami fizycznymi włącza powiadomienia informujące o problemach w działaniu dysków fizycznych w przypadku, gdy takie problemy są raportowane w systemie
- Pokazuj ostrzeżenia o kończących się zasobach włącza powiadomienia informujące o zbyt małych zasobach dostępnych dla systemu, np. w przypadku kończącego się miejsca na dysku
- 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" 2, 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

m mks vir Szvbka konfiguracia	O×
Tryb wydajny	
Tryb optymalny	
Tryb paranoiczny	
	Zamknij

 Ustawienia użytkownika – informacja pojawiająca się w przypadku, gdy aktualna konfiguracja programu mks\_vir nie odpowiada żadnemu z predefiniowanych profili

m mks vir Szybka konfiguracja	<u></u> >
✤ Tryb wydajny	
🖒 Tryb optymalny	
Tryb paranoiczny	
Service Servic	
Zamknij	

D – przywraca domyślną konfigurację programu mks\_vir (przywróć ustawienia domyślne)

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

Aby uaktualniać 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  $\rightarrow$  Aktualizacja"
  - 3. zaznaczamy opcje "Twórz repozytorium" i "Udostępnij repozytorium" oraz wpisujemy port np. 800:

- achrona	☑ Aktualizuj automatycznie
<b>V</b> ochrona	Serwer aktualizacji
skanowanie	Serwer: Serwer aktualizacji mks_vir
<b>^</b>	Opcje aktualizacji
kontrola rodzicielska	O Harmonogram aktualizacji
	Potwierdzaj aktualizację modułów programu
aktualizacja	Proxy
•	Użyj serwera proxy
ogólne	Repozytorium
	☑ Twórz repozytorium
	⊻Udostępnij repozytorium Port, na którym jest udostępnione repozytorium: 800
	Port, na którym jest udostępnione repozytorium: 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  $\rightarrow$  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):

m mks_vir		0_×
mks_Vır	ewersja bazy wirusów: 2023.03.06 12:13:44	Licencja: 667 dni
<b>O</b> ochrona	☑ Aktualizuj automatycznie Serwer aktualizacji	
	Serwer: Inny server Http	
kontrola rodzicielska	Opcje aktualizacji	
aktualizacja	Harmonogram aktualizacji Potwierdzaj aktualizację modułów programu	
🗙 ogólne	Proxy	
	□ Twórz repozytorium □ Udostępnij repozytorium	
	🖀 Q 🛡 📥 🖬 🌻 💆 🎤	<b>(i)</b>

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

Aby uaktualniać instalacje programu **mks\_vir** na stacjach bez dostępu do sieci za pomocą mechanizmu repozytorium przenoszonego na płycie 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  $\rightarrow$  Aktualizacja"
  - 3. zaznaczamy opcję "Twórz repozytorium":

m mks_vir	0 _>
mks_Vır	Se Wersja bazy wirusów: 2023.03.06 12:13:44 E Licencja: 667 dni
<b>U</b> ochrona	☑ Aktualizuj automatycznie Serwer aktualizacji
<b>Q</b> skanowanie	Serwer: Serwer aktualizacji mks_vir
kontrola rodzicielska	Opcje aktualizacji OHarmonogram aktualizacji
aktualizacja	□ Potwierdzaj aktualizację modułów programu Proxy
ogólne	□Użyj serwera proxy Repozytorium
	☑ Twórz repozytorium □ Udostępnij repozytorium
	👫 Q 🛡 🚣 📧 🌞 💆 ۶ 🕄

- 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  $\rightarrow$  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  $\rightarrow$  Zapora  $\rightarrow$  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
- Dopuść 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  $\rightarrow$  Kontrola urządzeń USB  $\rightarrow$  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
- **Dopuść** 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  $\rightarrow$  Kontrola urządzeń multimedialnych  $\rightarrow$  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  $\rightarrow$  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":

Emks vir Reguły zapory sieciowej	· · · · · · · · · · · · · · · · · · ·
Aplikacja	Reguła
C msedge.exe	
Dodaj aplikację Reguła systemowa	Zamknij

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

<sup>aks</sup> vir Reguły zapory sieciowej		0_
	Aplikacja	Reguła
C msedge.exe		
Dodaj aplikację Reguła	systemowa	Zamknij

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

nks. vir Reguły zapory siecio	wej	0.
	Aplikacja	Regula
C msedge.exe		
Dodaj aplikację	Reguła systemowa	Zamknij

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  $\rightarrow$  Kontrola urządzeń USB  $\rightarrow$  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):

		U.
zenie	Dostęr	
r/2023.07.04 08:44:23	Zablokuj	() () () () () () () () () () () () () (
07.04 08:44:15	Zablokuj	$\odot$
		Zamlunii
	zenie r/2023.07.04 08:44:23 07.04 08:44:15	zenle Dostęp r/2023.07.04 08:44:23 Zablokuj 07.04 08:44:15 Zablokuj

na akcję "Dopuść" (czyli zezwalającą na użycie danego urządzenia):

nks vir		0.
Lista reguł dla urządzen USB		
Urządzenie	Dostęp	
•↔ Intenso/Portable SSD/SCSIAdapter/2023.07.04 08:44:23	Dopuść	<ul> <li>•</li> <li>•</li></ul>
+ USB/ SanDisk 3.2Gen1/USB/2023.07.04 08:44:15	Zablokuj	• • ×
	1	
Dodaj urządzenie	Za	amknij
	/	

lub odwrotnie, z akcji "Dopuść" 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. Kolejość zdefiniowanych reguł można zmieniać za pomocą strzałek  $\uparrow i \downarrow$  (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak  $\otimes$  (również po prawej stronie).

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

Szczegóły urządze	nia USB
Etykieta urządzenia:	Intenso/Portable SSD/SCSIAdapter/2023.07.04 08:44:23
Producent:	=Intenso
Produkt:	=Portable SSD
Klasa:	=SCSIAdapter
Opis:	=USB Attached SCSI (UAS) Mass Storage Device
Numer seryjny:	=2017082715094
Wpisz dane identyfii zostaną automatycz ponownie.	kujące urządzenie lub podłącz go do portu USB. Po podłączeniu urządzenia pola nie uzupełnione. Jeśli urządzenie jest już podłączone, odłącz je i podłącz
ок	Anuluj

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):

nks vir	0
Szczegóły urządzei	hia USB
Etykieta urządzenia:	Urzadzenie USB
,	×
Producent:	
Produkt:	
Klasa:	
Opis:	
Numer seryjny:	
Wpisz dane identyfi zostaną automatycz ponownie.	cujące urządzenie lub podłącz go do portu USB. Po podłączeniu urządzenia pola nie uzupełnione. Jeśli urządzenie jest już podłączone, odłącz je i podłącz
<b>O</b> //	
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  $\rightarrow$  Kontrola urządzeń multimedialnych  $\rightarrow$  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):

	Aplikacja	Dostęp	
Skype.exe		Zablokuj	<ul> <li>♦ ♦ ∞</li> </ul>

na akcję "Dopuść" (czyli zezwalającą na dostęp):



lub odwrotnie, z akcji "Dopuść" 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. Kolejość zdefiniowanych reguł można zmieniać za pomocą strzałek  $\uparrow i \downarrow$  (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak  $\otimes$  (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  $\rightarrow$  Kontrola aplikacji  $\rightarrow$  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):

Links vir Lista reguł dla aplikacji			8
Proces nadrzędny (uruchamiający)	Aplikacja	Dostęp	
		Zablokuj	<ul> <li>The second second</li></ul>
Dodaj regułę		Zar	nknij
		~ U	

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 ("Dopuść"), 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 ("Dopuść")

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:

m mks. vir Lista reguł dla aplikacji		©_>
Proces nadrzędny (uruchamiający)	Aplikacja	Dostęp
	myapp.exe	Dopuść 💿 🔄 😒
Dodaj regułę		Zamknij

• 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:

mo	ıks vir Lista reguł dla aplikacji		0_>
Ŀ	Proces nadrzędny (uruchamiając	y) Aplikacja	Dostęp
L	myappmaster.exe	myapp.exe	Zablokuj 💿 🏵 😒
L			
L			
L			
	Dodai rogulo		Zamkaii
L			Zanknj

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. Kolejość zdefiniowanych reguł można zmieniać za pomocą strzałek  $\uparrow i \downarrow$  (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak  $\otimes$  (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  $\rightarrow$  Pokaż listę reguł użytkownika":



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



Aby utworzyć własną regułe 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:

m mks vir Lista reguł użytkownika			@_×
Reguła	Zakres	Akcja	
	Adres	Blokuj	${}{}{}{}{}{}{}$
Dodaj regułę		2	Zamknij
		_	_

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. Kolejość zdefiniowanych reguł można zmieniać za pomocą strzałek  $\uparrow i \downarrow$  (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak  $\otimes$  (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  $\rightarrow$  Pokaż historię przeglądanych stron":

Adres	Czas	A	kcja	/
msn.com	2020.12.15 12:32:34	Pozwól	Blokuj	1
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	Pozwól	Blokuj	
trackmytarget.com	2020.12.15 12:32:44	Pozwól	Blokuj	
wp.pl	2020.12.15 12:32:40	Pozwól	Blokuj	
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	Pozwól	Blokuj	
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	`

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
oushpushgo.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

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	

### Jak dodać domenę internetową do wykluczeń

Instrukcja ta umożliwia 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":

m mks_vir	0_×
mks_Vır	Se Wersja bazy wirusów: 2020.12.15 11:20:33
U ochrona	Chroń hasłem ustawienia pakietu mks_vir Ostawienia szczegółowe
skanowanie	Globalne wykluczenia ochrony
$\sim$	Lista wykluczonych domen internetowych
kontrola	C Lista wykluczonych plików i folderów
rodzicielska	Porty i protokoły
🚽 aktualizacja	Tabela skanowanych i wykluczonych portów i protokołów
	Folder danych
ogólne ogólne	Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zapasowe, szyfrowane dyski.
	☑ Korzystaj z domyślnego folderu danych pakietu mks_vir
	Importuj ustawienia Eksportuj ustawienia Przywróć ustawienia domyślne

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

n mks vir O	$ \ge \times $
Lista wykluczonych domen internetowych	
Domena	
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
	- 8
Dodaj domenę Zamknij	
	_

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":

n mks vir	<u> </u>
Lista wykluczonych domen internetowych	
Domena	
men.gov.pl	( )
l	
Dodaj domenę	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 umożliwia 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":

m mks_vir		0_X
mks_Vır	Service Se	ni
U ochrona	Chroń hasłem ustawienia pakietu mks_vir Ustawienia szczegółowe	
	Globalne wykluczenia ochrony	
$\sim$	Lista wykluczonych domen internetowych	
kontrola	Lista wykluczonych plików i folderów	
n rodzicielska	Porty i protokoły	
🚽 aktualizacja	Tabela skanowanych i wykluczonych portów i protokołów	
	Folder danych	
ogólne ogólne	Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zapasowe, szyfrowane dyski.	
	🗹 Korzystaj z domyślnego folderu danych pakietu mks_vir	
	Importuj ustawienia Eksportuj ustawienia Przywróć ustawienia	domyślne
	🛞 Q 🗊 🕹 🖂 🧌 🕅 🔎 A	

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

Lista wykluczonych plików i folderów Pliki / Foldery Dodaj plik Dodaj folder Zamknij	n mks vir	0	×
Pilki / Foldery	Lista wykluczonych plików i folderów		
Pilki / Foldery Dodaj plik Dodaj folder Zamknij			
Pliki / Foldery Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij	Pliki / Foldery		
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
Dodaj plik Dodaj folder Zamknij			
	Dodaj plik Dodaj folder Zamknij		

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 wykluczany jest folder) i klikając "OK":

Przeglądanie w poszukiwaniu folderu	$\times$
System32	^
0409	
AdvancedInstallers	
af-ZA	
am-ET	
AppLocker	
appraiser	
AppV	
ar-SA	~
Utwórz nowy folder OK Anuluj	

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

m mks vir Lista wykluczonych plików i folderów	@×
Pliki / Foldery	
C:\Windows\System32\	$\odot$
	I
	I
Dodaj plik Dodaj folder	Zamknij

# Jak dodać proces do wykluczeń

Instrukcja ta umożliwia 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":

m mks_vir	0_×
mks_Vır	Se Wersja bazy wirusów: 2021.12.07 07:26:46 E Licencja: 64 dni
U ochrona	Chroń hasłem ustawienia pakietu mks_vir Ostawienia szczegółowe
	Giobalne wykluczenia ochrony
$\sim$	Lista wykluczonych domen internetowych
♥       ochrona       □ Chroń hasłem         ♥       skanowanie       □ Ustawienia szcz         ♥       skanowanie       □ Lista wykluczou         ●       Lista wykluczou       □ Lista wykluczou         ●       Lista wykluczou       □ Lista wykluczou         ●       aktualizacja       Porty i protokoły         ●       ogólne       Folder danych	Lista wykluczonych plików i folderów
♥ ochrona       □ Chroń hasłem ustawienia pakietu mks_vir         ● Ustawienia szczegółowe         ● Ustawienia szczegółowe         ● Obalne wykluczenia ochrony         ● Lista wykluczonych domen internetowych         ● Lista wykluczonych pilków i folderów         ● Lista wykluczonych procesów         ● Drty i protokoły         ● Tabela skanowanych i wykluczonych portów i protokołów         Folder danych	
<ul> <li>kontrola rodzicielska</li> <li>Lista v</li> <li>Lista v</li> <li>Lista v</li> <li>Lista v</li> <li>Lista v</li> <li>Tabel</li> <li>ogólne</li> </ul>	Porty i protokoły
♥ ochrona       □ Chroń hastem ustawienia pakietu mks_vir         ● Ustawienia szczegółowe         ● Ustawienia szczegółowe         ● Ustawienia szczegółowe         ● Obalne wykluczenia ochrony         ● Lista wykluczonych domen internetowych         ● Lista wykluczonych pilków i folderów         ● Lista wykluczonych procesów         ▶ aktualizacja         ▶ ogólne         Folder danych         ▶ Lista wykluczonych i wykluczonych portów i protokołów	
ogólne	Folder danych
	Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zapasowe, szyfrowane dyski.
	☑ Korzystaj z domyślnego folderu danych pakietu mks_vir
	Importuj ustawienia Eksportuj ustawienia Przywróć ustawienia domyślne
	希 Q 🛡 📩 🖬 🌞 🔂 🗲 🕄

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

m mks vir	<u> </u>
Lista wykluczonych procesów	_
	_
Á staður annar	- 1
Scieżka procesu	- 1
	- 1
	- 1
	- 8
Dodaj ścieżkę procesu Dodaj nazwę procesu Zamknij	

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

→ * ↑ <mark>-</mark> «	▶ 🧧 « Dysk lokalny (C:) → Program Files → totalcmd 🗸		, Ö , Przes	zukaj: totalcmd	
ganizuj 🔻 Nowy	folder				?
	Nazwa	Data modyfikacji	Тур	Rozmiar	
<ul> <li>Szybki dostęp</li> </ul>	FILTER64	01.12.2021 12:19	Folder plików		
Pulpit 🤉	LANGUAGE	01.12.2021 12:19	Folder plików		
🖊 Pobrane 🛛 🤅	NOCLOSE.EXE	10.06.2021 11:00	Aplikacja	51 KB	
Dokumenty	NOCLOSE64.EXE	10.06.2021 11:00	Aplikacja	59 KB	
	SHARE_NT.EXE	10.06.2021 11:00	Aplikacja	3 KB	
oblazy	TCMADM64.EXE	10.06.2021 11:00	Aplikacja	115 KB	
OneDrive	🔯 TCMADMIN.EXE	10.06.2021 11:00	Aplikacja	86 KB	
Ten komputer	TCMDX32.EXE	10.06.2021 11:00	Aplikacja	90 KB	
len komputer	TCMDX64.EXE	10.06.2021 11:00	Aplikacja	124 KB	
Sieć	🔀 TCUNIN64.EXE	10.06.2021 11:00	Aplikacja	101 KB	
	🔀 TCUNINST.EXE	10.06.2021 11:00	Aplikacja	53 KB	
	💾 TcUsbRun.exe	10.06.2021 11:00	Aplikacja	58 KB	
	TOTALCMD.EXE	10.06.2021 11:00	Aplikacja	5 221 KB	
	TOTALCMD64.EXE	10.06.2021 11:00	Aplikacja	9 598 KB	
	WC32TO16.EXE	10.06.2021 11:00	Aplikacja	4 KB	
Na	zwa pliku: TOTALCMD.EXE		<ul> <li>Pliki wyko</li> </ul>	nywalne (*.exe)	~

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

iks vir Lista wykluczonych procesów		0
	Ścieżka procesu	
C:\Program Files\totalcmd\TOTA	() () ()	
Dodaj ścieżkę procesu	Dodaj nazwę procesu	Zamknij

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

# Jak dodać porty do wykluczeń

Instrukcja ta umożliwia 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":

m mks_vir	<b>0</b> _×
mks_Vır	See Wersja bazy wirusów: 2020.12.15 11:20:33 E Licencja: 421 dni
U ochrona	Chroń hasłem ustawienia pakietu mks_vir     Ustawienia szczegółowe
	Globalne wykluczenia ochrony
$\sim$	Lista wykluczonych domen internetowych
🔶 kontrola	Lista wykluczonych plików i folderów
rodzicielska	Porty i protokoły
上 aktualizacja	Tabela skanowanych i wykluczonych portów i protokołów
	Folder danych
ogóine ogóine	Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zapasowe, szyfrowane dyski.
	☑ Korzystaj z domyślnego folderu danych pakietu mks_vir
	Importuj ustawienia Eksportuj ustawienia Przywróć ustawienia domyślne
	🔺 Q U 🚣 📼 🌻 🗗 ۶ 🚯

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

nks vir	_	_	_	_	_	0_
Tabela skanowany	ch i wykluczony	ch portów i p	rotokołów			
Wpisz porty oddzie	lając je przecinkan	<i>īi.</i>				
Porty i protokoly sk	20000200					
	anowane					
Dostęp do listy port	tów jest dostępny	tylko przy nieał	tywnej zaporze	e sieciowej.		
Porty wykluczone						
Porty wykluczone:						
					Zamknij	

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:

Wpisz porty oddzielając je przecinkami.					
Porty i protokoły sł	inowane				
Dostęp do listy por	ów jest dostępny tylko przy nieaktywnej zaporz	re sieciowej.			
Porty wykluczone					
Porty wykluczone:	8008,8009				

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:



- 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

e-mail kontaktowy:	moj email@moja.domena		
,			
emat wiadomości:	Problem		
viadomość / opis problemu:	Opis problemu	 	
oliki do wysłania / załączniki:	Dodaj plik		
👖 C:\ProgramData\mks_vir\logs\20	201215\arcadump-20201215121524.zip		)

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:

m mks_vir rescue disk generator	- 0	×
<b>mks_VIF</b> RESCUE DISK	K	
Obraz ISO		
<ul> <li>Pobierz aktualny obraz ISO z serwera firmy mks_vir</li> </ul>		
○ Wskaż plik z obrazem ISO		
Nośnik do zapisu		
D:\ [ USB SanDisk 3.2Gen1 USB Device - (14660,88 MB)]		$\sim$
	Generuj Rescue Disk	

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:

Trwa generowanie Rescue Disk	×
Pobieranie obrazu ISO z serwera firmy mks_vir	
	Anuluj

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

Uwaga		×
Wszystkie dane na wybranym noś kontynuować?	niki zostaną usunięte. Czy chcesz	
	Tak <u>N</u> ie	

Po kliknięciu "Tak" rozpocznie się właściwe tworzenie nośnika ratunkowego:

Trwa generowanie	Rescue Disk	
Generowanie R	escue Disk	
		Anuluj

Gdy tworzenie zakończy się, pojawi się stosowny komunikat informujący, że nosnik ratunkowy "Rescue Disk" jest gotowy:

	×
Rescue Disk został wygenerowanj	y.
ОК	

## 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 zależne 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 "Usuń zagrożenia":



Po wybraniu *"Usuń 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  $\rightarrow$  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" umożliwia utworzenie szyfrowanego dysku i dostosowanie jego parametrów:

Nazwa dysku:	szyfrowany dysk 20180110151240	
Rozmiar dysku:	1 GB 🗸	
Hasło:		
Powtórz hasło:		

- 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):

Rozmiar dysku:	szyfrowany dysk 20180110151240 512 MB 1 GB	
Hasło:	2 GB 4 GB 8 GB 16 GB 32 GB 6 4 GB	
Powtórz hasło:		

 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*:

<b>mks_VIF</b> SZYFROWANE DYSKI	0_X
<u> </u>	
Nie iest dostepny żaden szyfrowany dysk.	
Proszę czekać, trwa tworzenie dysku	
Pokaż konsolę szyfrowanych dysków po zalogowaniu Stwórz nowy szyfrowan	ny dysk

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
- ② umożliwia skasowanie *szyfrowanego dysku* (skasowanie dysku powoduje fizyczne usunięcie pliku dysku wraz z zawartymi na nim danymi, co uniemożliwia ich ew. odzy-skanie)

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

<b>mks_VIF</b> SZYFROWANE D'	YSKI
F: Szyfrowany dysk 20180110151240	1 GB 🔗 🛞
Podłączanie dysku - hasło	
Podaj hasło dla dysku: szyfrowany dysk 201801101512	40
 ☑ Podłącz dysk tylko dla mnie	2
Anuluj F	Podłącz dysk
Pokaż konsolę szyfrowanych dysków po zalogowaniu	Stwórz nowy szyfrowany dysk

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  $\rightarrow$  Menadżer haseł" w głównym oknie:

	IV3_A11		Jazy Wirusow. 2022.	03.04 10.23.30 <b>∎</b> ≡	Licencja, 575 dni
Na	rzędzia				
	<b>^</b>	â		മ്പ	
	Kwarantanna	SafeStorage	Bezpieczna przeglądarka	Kopie zapasowe	Menadžer procesów
	<u>.111</u>		٢	4	<b>B</b>
	Audyt systemu	Rescue Disk	Czyszczenie systemu	Windows Update	Wsparcie online
	Q.	*		<b>.</b> #	~
	Szyfrowane dyski	Menadżer haseł	Zarządzanie pakietem	Konsola administracyjna	Wydajność systemu

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 zaznaczyliśmy opcję "Stwórz plik z dodatkowym kluczem zabezpieczającym bazę", także zapisanie pliku z dodatkowym kluczem zabezpieczającym:

m mks_vir - menadżer haseł	· · · · · · · · · · · · · · · · · · ·		-	×
	- <b>K</b> -	0		
		X		
		tester		
	Ustaw i potwierdź	nowe hasło do swojej bazy:		
r.				
	Stwórz plik z dodatkov	vym kluczem zabezpieczającym bazę		
	Ustaw hasło	Anuluj		

 
 • — importuj swoją bazę – umożliwia wczytanie swojej bazy danych z uprzednio zapamiętanej kopii zapasowej pliku bazy

W przypadku, gdy baza *menadżera haseł* została już wcześniej utworzona, zostanie otwarte okno umożliwiające podanie hasła zabezpieczającego dostęp do danych zgromadzonych w *menadżerze haseł* – 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":

mks_vir - menadžer haseł			-	×
<b>A</b> +	8	*		
	tester			
	Podaj hasło do swojej bazy:			
	Mam plik z dodatkowym kluczem zabezpieczającym bazę			
	Wczytaj bazę			

Dodatkowe ikony umożliwiają:

 A – 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):

Resetowanie bazy		
Uwaga! Resetowanie bazy usuwa całą jej zawartość i jest procesem nieodwracalnym!		
Żeby zresetować bazę musisz posladać <b>jednorazowy kod</b> , który możesz uzyskać wysyłając email na adres pomoc@mks-vir.pl. Pamiętaj, że adres z którego wyślesz email musi być taki sam jak ten, który był wykorzystany przy zakupie programu.		
Jeśli posiadasz już kod, wpisz go w poniższym polu i naciśnij przycisk 'Resetuj bazę'.		

 
 • — importuj swoją bazę – umożliwia wczytanie swojej bazy danych z uprzednio zapamiętanej kopii zapasowej pliku bazy

m mks_vir - menadže	r hasel	-	×
ĺ	Menadżer haseł - pytanie		
	Import bazy spowoduje usunięcie zawartości aktualnej bazy. Jest to proces nieodwracalny!		
	Czy chcesz kontynuować?		
	Tak Nie		
, l			

- • ygeneruj 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:

m mks_vir - menad	zer hase <del>l</del>			×
	Generacja	nowego hasła		
	Zestaw dost	ępnych znaków		
	☑ Wielkie litery (A, B, C) ☑ Małe litery (a, b, C) ☑ Cyfry(0, 1, 2) ☑ Myślnik i podkreślenie ()	□ Spacja ☑ Znaki specjalne (!, @, #, \$, %) □ Nawiasy i klamry ( [, ], (, })		
	Długo	ość hasła		
	$\odot$	20 🕣		
	Twoje r	owe hasło		
	1ab4XAdFr	1X95K!7g%aap		
	Wykorzystaj hasło	Anuluj		

Pierwsze otwarcie bazy danych menadżera haseł wyświeli 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*:

m mks_vir - menadžer haseł				-		×
			_		_	
Tytuł/Nazwa:						
Użytkownik:			6 <b>6</b> 2			
Hasło:		*	: 👁 ★	ß		
URL (adres):		ଜ	>			
	ui/Nazwa: /tkownik: sło: L (adres): Notatki					
	Notati	ki .				
						ן
Zapisz		[		Anuluj		ן
						ر 

- 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 konkretmej 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:

m mks_vir - m	enadžer hasel		-		×
A test		•	•	*	C
	Generacja nowego hasła				
	Zestaw dostępnych znaków				
	Wielkie litery (A, B, C)     □ Spacja     Małe litery (a, b, c)     Znaki specjalne (!, @, #, \$, %)     Cyfry(0, 1, 2)     Nawiasy i klamry ( [, ], {, })     Myślnik i podkreślenie ()				
	Długość hasła				
	⊙ 20 ⊙				
	Twoje nowe hasło •kdl5QUD^ikJpKKeV_PX				
	Wykorzystaj hasło Anuluj				

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

mks_vir - menadžer haseł		-	×
		_	
⇒	8		
	tostor		
	tester		
	Ustaw i potwierdź nowe hasło do swojej bazy:		
	$\Box$ Stwórz plik z dodatkowym kluczem zabezpieczającym bazę		
	Ustaw hasło Anuluj		

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



Poszczególne ikony widoczne po prawej stronie paska danego wpisu umożliwiają:

- Otwórz stronę otwiera stronę www zdefiniowanej usługi w domyślnej przeglądarce internetowej
- Kopiuj nazwę uzytkownika kopiuje nazwę użytkownika dla zdefiniowanej usługi do schowka systemowego
- Kopiuj hasło kopiuje hasło dla zdefiniowanej usługi do schowka systemowego
- Kopiuj 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:

mks_vir - menadżer haseł		- 🗆 X
Tytuł/Nazwa:	Mój bank	
Użytkownik:	login_bankowy	<b>a</b> 2
Hasło:	•••••	* 👁 ★ 🗹
URL (adres):	https://adresbanku.pl/	00
	Notatki	
Dane logujące do mojego	banku.	
Zapisz		Anuluj

## 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:

📘   🕑 📑 ᆕ		Zarządzanie bin		-	п х
Plik Narzędzia główne	Udostępnianie Widok	Narzędzia aplikacji			~ 😲
🔶 🔶 👻 🛧 📙 « Pro	gram Files → mks_vir → bin →		Przeszukaj: bin		
<b>a</b>	Nazwa	Data modyfikacji	Тур	Rozmiar	^
Szybki dostęp	nss	26.11.2019 09:13	Folder plików		
Pulpit 🖈	7z.dll	26.11.2019 09:13	Rozszerzenie aplik	1 571 KB	
🔶 Pobrane 🛛 🖈	7z.exe	26.11.2019 09:13	Aplikacja	447 KB	
🛄 Ten komputer	🗟 abck.dll	26.11.2019 09:13	Rozszerzenie aplik	2 749 KB	
	限 ac.exe	26.11.2019 09:16	Aplikacja	100 KB	
💣 Sieć	🗟 acomm.dll	26.11.2019 09:16	Rozszerzenie aplik	3 017 KB	
	🗟 ail.dll	26.11.2019 09:13	Rozszerzenie aplik	2 677 KB	
	m amcmd.exe	26.11.2019 09:16	Aplikacja	71 KB	
	📄 andapk01.dat	26.11.2019 09:12	Plik DAT	23 KB	
	📄 android.dat	26.11.2019 09:12	Plik DAT	41 KB	
	🗟 arcael.sys	26.11.2019 09:13	Plik systemowy	17 KB	
	📄 arcafsav.bin	26.11.2019 09:12	Plik BIN	2 KB	
	🗟 arcafsav.sys	26.11.2019 09:13	Plik systemowy	27 KB	
	🗟 arcafsav10.sys	26.11.2019 09:13	Plik systemowy	44 KB	
	🗟 arcamag.dll	26.11.2019 09:13	Rozszerzenie aplik	2 746 KB	
	🗟 arcasd.dll	26.11.2019 09:13	Rozszerzenie aplik	523 KB	
	🗟 arcasd.sys	26.11.2019 09:13	Plik systemowy	246 KB	
	arcasd1.sys	26.11.2019 09:13	Plik systemowy	227 KB	
	arcausb.sys	26.11.2019 09:13	Plik systemowy	108 KB	
	arcawfp.sys	26.11.2019 09:13	Plik systemowy	65 KB	
	arcawfp1.sys	26.11.2019 09:13	Plik systemowy	57 KB	~
Elementy: 106 1 zaznaczo	ony element. 70,0 KB				

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			-	$\times$
C:\Users\tester>"c:\Program Files\mks_vir\bi c:\Users\tester\Desktop\test\0000000.vir c:\Users\tester\Desktop\test\000000000.vir c:\Users\tester\Desktop\test\0000000000000000000000000000000000	n\amcmd.exe" c:\ INFECTED INFECTED INFECTED INFECTED INFECTED INFECTED INFECTED INFECTED INFECTED	Users\tester\Desktop\test Win32.Worm.Allaple.Gen Trojan.Generic Trojan.A Trojan.A Trojan.A Win32.Worm.Allaple.Gen Win32.Worm.Allaple.Gen 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):

<sup>&</sup>quot;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 -	$\times$
	^
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.\lisans\tastan\	
	~

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:/l	sers\tester>"c:\Program Files\mks_vir\bi	n\amcmd.exe" c	:\Users\tester\Desktop\test /delete		
c:\(	sers\tester\Desktop\test\00000001.vir	INFECTED	Win32.Worm.Allaple.Gen DELETED		
c:\l	<pre>sers\tester\Desktop\test\00000002.vir</pre>	INFECTED	Trojan.Generic DELETED		
c:\(	<pre>sers\tester\Desktop\test\00000003.vir</pre>	INFECTED	Trojan.Generic.D279B6F6 DELETED		
::\(	<pre>lsers\tester\Desktop\test\0000004.vir</pre>	INFECTED	Trojan.A DELETED		
::\(	sers\tester\Desktop\test\00000005.vir	INFECTED	Trojan.A DELETED		
::\(	<pre>sers\tester\Desktop\test\0000006.vir</pre>	INFECTED	Win32.Worm.Allaple.Gen DELETED		
::\(	<pre>sers\tester\Desktop\test\00000007.vir</pre>	INFECTED	Win32.Worm.Allaple.Gen DELETED		
c:\l	sers\tester\Desktop\test\0000008.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:



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  $\rightarrow$  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 jakiś powodów 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:

mks_vir Safe Browser				-		×
mks_Vır						
Nie wszystkie	moduły c	ochronne szczególnie is	stotne dla pracy b	ezpiec	znej	
p	rzeglądari	ki są aktywne. Zalecam	iy ich aktywację.			
	_		_			
	U	Ochrona plików				
	¢,	Ochrona przeglądarki				
	A	Zapora sieciowa	$\bigcirc$			
						٦

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 przegądarki internetowe oraz programy do zdalnego dostępu):

m mks_vir Safe Browser		-	×
mks_Vır			
Przed uruchomieniem przeglądarki zale	camy zamknięcie następujących aplikacji:		
C:\Program Files (x86)	Microsoft/Edge/Application/msedge.e	xe	
	Zamknij zaznaczone aplikacje i kontynuuj	<b>→</b>	]

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:

m mks_vir	Safe Browser	-	×
mks.	_Vir		
🕀 No	wy adres		
	Uruchom przeglądarkę mks_vir Safe Browser		
	Nowy adres		
	Anuluj Dodaj		

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)
- C 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 zdefiniowanych 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 definiowac 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:

······································		
Kopia zapasowa		
Foldery źródłowe		
Folder		Dodaj folder
C:\Users\tester\Pictures\	( () ())	
C:\Users\tester\Music\		
C:\Users\tester\Videos\	$( \blackblackblackblackblackblackblackblack$	
Ustawienia		
Archiwizuj tylko pliki nowe i zmienione <i>(kopia przyro</i>	ostowa)	
🕽 Harmonogram kopii zapasowej		
🕽 Ustawienia zaawansowane		

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:

KS VII		
Zaawansowane ustawienia kopii zapas	sowej	
	-	
Typy plików		
Wszystkie pliki		
✓ Dokumenty		
✓ Pliki graficzne		
✓ Pliki audio		
✓ Pliki wideo		
Kody źródłowe		
nne <i>(maski plików)</i> .		
Folder konji zanasowaj		
FOIDEL KODII ZADASOWEI		
Folder dla kopii zapasowej <i>(puste pole ozna</i>	acza folder domyślny).	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny). Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny). Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny). Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny). Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny). Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder dla kopil zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder dla kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	
Folder (la kopii zapasowej <i>(puste pole ozna</i> D:\	acza folder domyślny): Wskaż folder	Zapisz

- \* **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:

- <br/>  ${\ensuremath{ \ensuremath{ \ensure$
- 🚯 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:

п Коріа заразоwа		– 🗆 X
mks_Vır		Kopia zapasowa (4)
Filtr:	¢	
Ścieżka	Plik	Data archiwizacji
C:\Users\tester\Pictures\01.png	01.png	2019-10-01 14:53:00
C:\Users\tester\Pictures\02.png	02.png	2019-10-01 14:53:00
C:\Users\tester\Pictures\03.png	03.png	2019-10-01 14:53:00
C:\Users\tester\Pictures\04.png	04.png	2019-10-01 14:53:00
Odzyskaj		Zamknij

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

Odtworzenie plików z	e wskazanej wersji kopii zapasowej
W tym trybie zostana oo	łtworzone pliki ze wskazanej wersji kopii zapasowej:
2019-10-01 14:53:00	~
Odtworzonio wczystki	sh njikáu
	theoryone wszystkie wersie plików zarchiwizowane w
kopii zapasowej. Do naz	wy kazdego pliku zostanie dodana data jego archiwizacji.

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

Przeglądanie w poszukiwaniu folderu	×
Wybierz folder dla odzyskanych plików	
Pulpit	
> 🦱 OneDrive	
> 🤱 tester	
> 💻 Ten komputer	
> 🐂 Biblioteki	
> 💣 Sieć	
> 🖭 Panel sterowania	
🛛 Kosz	
Eolder: Pulpit	
Utwórz nowy folder OK Anuluj	

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

Pilk       Narzędzia główne       Udostępnianie       Widok       Narzędzia obrazów            ←         →           Ten komputer         →         Pulpit         →         C           Ten komputer         Pulpit         →         C         Oata        Typ         Przeszukaj: pictures             Narzwa           Data           Typ           Rozmiar           Tagi             Szybki dostęp           Narzwa           Data           Typ           Rozmiar           Tagi             Pulpit           Potrane           O1.10.2019 11:35           Plik PNG           42 KB             Pobrane           O3.png           01.10.2019 11:35           Plik PNG           27 KB             Dokumenty           @         04.png           01.10.2019 11:38           Plik PNG           19 KB             ©         Ohrazy           #           O4.png           O1.10.2019 11:38           Plik PNG           19 KB             OneDrive           E ten komputer           E           E	$\times$		-	-		Zarządzanie		pictures	📊   🛃 📙 🖛
<ul> <li>← → · ↑ </li> <li>Ten komputer → Pulpit → c → users → tester → pictures</li> <li>✓ Ø</li> <li>Przeszukaj: pictures</li> <li>Rozmiar</li> <li>Tagi</li> <li>Ol.10.2019 11:35</li> <li>Plik PNG</li> <li>42 KB</li> <li>Ø 02.png</li> <li>01.10.2019 11:35</li> <li>Plik PNG</li> <li>14 KB</li> <li>Ø 03.png</li> <li>01.10.2019 11:37</li> <li>Plik PNG</li> <li>27 KB</li> <li>Ø 04.png</li> <li>01.10.2019 11:38</li> <li>Plik PNG</li> <li>9 KB</li> </ul>	~ ?					Narzędzia obrazów	Udostępnianie Widok	zia główne	Plik Narzędz
Nazwa       Data       Typ       Rozmiar       Tagi	ρ		ictures	Przeszukaj: pictur	~ Ū	s → tester → pictures	n komputer > Pulpit > c > use	> Ter	$\leftarrow \rightarrow \cdot \cdot \uparrow$
Image: Splick doskup       Image: Ol.png       01.0.2019 11:35       Plik PNG       42 KB         Image: Pulpit       Image: Ol.png       01.10.2019 11:35       Plik PNG       14 KB         Image: Pobrane       Image: Ol.png       01.10.2019 11:37       Plik PNG       27 KB         Image: Dokumenty       Image: Ol.png       01.10.2019 11:37       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       01.10.2019 11:38       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       01.10.2019 11:38       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       01.10.2019 11:38       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       01.10.2019 11:38       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       01.10.2019 11:38       Plik PNG       19 KB         Image: Obrazy       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png         Image: Obrazy       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png         Image: Obrazy       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png       Image: Ol.png		igi	r Ta	Rozmiar	Тур	а	Nazwa Dat		🗲 Szubki doste
Image: Spring of the poly of the p			42 KB	42 KB	Plik PNG	0.2019 11:35	01.png 01.1	۳ پ	Pulnit
♥ Potrane         Image: Windows Constraints         Potrane         Image: Windows Constraints         Pik PNG         27 KB           Image: Dokumenty         Image: Windows Constraints         Image: Windows Constra			I4 KB	14 KB	Plik PNG	0.2019 11:35	🖬 02.png 01.1	<i></i>	
Dokumenty * 04.png 01.10.2019 11:38 Plik PNG 19 KB Obrazy * OneDrive Ten komputer Biblioteki			27 KB	27 KB	Plik PNG	0.2019 11:37	🖬 03.png 01.1	R	🔶 Pobrane
■ Obrazy ★ OneDrive ■ Ten komputer Biblioteki ■ Sizé			19 KB	19 KE	Plik PNG	0.2019 11:38	<b>04.png</b> 01.1	y ≉	🔮 Dokument
OneDrive     Ten komputer     Biblioteki     Sinf								*	E Obrazy
Ten komputer									less oneDrive
Riblioteki								er	💻 Ten komput
Cin4									🐂 Biblioteki
Siec									💣 Sieć
Elementy: 4									Elementy: 4

# 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

🕴 🗹 🚽 Zesta	awien	ia		-	- 🗆 X
Plik Narzędzia gł	ówne	Udostępnianie Widok			~ 🕐
← → ✓ ↑ → Zestawienia ✓ ♂ Przeszukaj: Zestawienia					
		Nazwa	Data modyfikacji	Тур	Rozmiar
✓ ★ Szybki dostęp		Sprawozdanie 2018-01.docx.encrypted	09.01.2018 13:35	Plik ENCRYPTED	5 KB
Pulpit	×	Zestawienie 2013.docx.encrypted	09.01.2018 13:32	Plik ENCRYPTED	5 KB
Dokumenty	A	Zestawienie 2014.docx.encrypted	09.01.2018 13:33	Plik ENCRYPTED	5 KB
> 💪 OneDrive		Zestawienie 2015.docx.encrypted	09.01.2018 13:33	Plik ENCRYPTED	5 KB
		Zestawienie 2016.docx.encrypted	09.01.2018 13:09	Plik ENCRYPTED	5 KB
> 💻 Ten komputer		Zestawienie 2017.docx.encrypted	09.01.2018 13:34	Plik ENCRYPTED	5 KB
> 🛖 Dysk lokalny (D:)					
> 💣 Sieć					
> 🔩 Grupa domowa					
Elementy: 6					

Właśnie dla ochrony danych w takich przypadkach został wprowadzony mechanizm **Safe-Storage**. 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 zawartoścą *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

m SafeStorage			-		×
mks_Vır			SafeSto	orage	(14)
Filtr:	$\bigcirc$				
	Ścieżka	Plik	Data mo	dyfikac	ji
✓ c:\users\tester\	desktop\zestawienia\sprawozdanie 2018-01.doc	sprawozdanie 2018	2018.01.09	13:34	:55
✓ c:\users\tester\	desktop\zestawienia\sprawozdanie 2018-01.doc	sprawozdanie 2018	2018.01.09	13:34	:56
✓ c:\users\tester\	desktop\zestawienia\sprawozdanie 2018-01.doc	sprawozdanie 2018	2018.01.09	13:34	:58
✓ c:\users\tester\	desktop\zestawienia\sprawozdanie 2018-01.doc	sprawozdanie 2018	2018.01.09	13:35	:00
✓ c:\users\tester\	desktop\zestawienia\sprawozdanie 2018-01.doc	sprawozdanie 2018	2018.01.09	13:35	:02
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2013.docx	zestawienie 2013.d	2018.01.09	13:33	:35
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2014.docx	zestawienie 2014.d	2018.01.09	13:34	:03
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2015.docx	zestawienie 2015.d	2018.01.09	13:34	:12
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2016.docx	zestawienie 2016.d	2018.01.09	13:34	:24
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2017.docx	zestawienie 2017.d	2018.01.09	13:34	:37
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2017.docx	zestawienie 2017.d	2018.01.09	13:34	:38
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2017.docx	zestawienie 2017.d	2018.01.09	13:34	:40
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2017.docx	zestawienie 2017.d	2018.01.09	13:34	:42
✓ c:\users\tester\	desktop\zestawienia\zestawienie 2017.docx	zestawienie 2017.d	2018.01.09	13:34	:44
Odzyskaj	Usuń z bazy Usuń nie	stniejące		Zamkn	ij

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

Przeglądanie w poszukiwaniu folderu	×
Wybierz folder dla odzyskanych plików	
> 💻 Ten komputer	^
> 🍃 Biblioteki	
> 🚔 Dysk lokalny (D:)	
> 💣 Sieć	
> 🔩 Grupa domowa	
> 🖭 Panel sterowania	
🔊 Kosz	
🔄 odzyskane	
	¥
Eolder: odzyskane	
Utwórz nowy folder OK Anuluj	

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

	> users > tester > desktop > zestawienia	v ö	Przeszukai: zestawie	nia
	Nazwa	Data modvfikacij	Typ	Rozmiar
📌 Szybki dostęp	sprawozdanie 2018-01.docx	09.01.2018 13:43	Dokument Micros	5 KB
🔜 Pulpit 🛛 🖈	sprawozdanie 2018-01-001.docx	09.01.2018 13:43	Dokument Micros	5 KE
🔮 Dokumenty 🛛 🖈	i sprawozdanie 2018-01-002.docx	09.01.2018 13:43	Dokument Micros	5 KE
📰 Obrazy	📄 sprawozdanie 2018-01-003.docx	09.01.2018 13:43	Dokument Micros	5 KE
a OneDrive	📄 sprawozdanie 2018-01-004.docx	09.01.2018 13:43	Dokument Micros	5 KE
	📄 zestawienie 2013.docx	09.01.2018 13:43	Dokument Micros	5 KE
💻 Ten komputer	📄 zestawienie 2014.docx	09.01.2018 13:43	Dokument Micros	5 KE
<ul> <li>Dvsk lokalny (D:)</li> </ul>	📄 zestawienie 2015.docx	09.01.2018 13:43	Dokument Micros	5 KE
	📄 zestawienie 2016.docx	09.01.2018 13:43	Dokument Micros	5 KE
💣 Sieć	📄 zestawienie 2017.docx	09.01.2018 13:43	Dokument Micros	5 KE
🔩 Grupa domowa	📄 zestawienie 2017-001.docx	09.01.2018 13:43	Dokument Micros	5 KE
•	📄 zestawienie 2017-002.docx	09.01.2018 13:43	Dokument Micros	5 KE
	📄 zestawienie 2017-003.docx	09.01.2018 13:43	Dokument Micros	5 KE
	📄 zestawienie 2017-004.docx	09.01.2018 13:43	Dokument Micros	5 KE

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 miejscem 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:

m mks_	vir - czyszczenie systemu	- 🗆 X
m	ks_Vır	CZYSZCZENIE SYSTEMU
<b>P</b>	TEST01	Miejsce do odzyskania: 517.3 MB
U	Tymczasowe pliki oprogramowania antywirusowego	500.72 MB
-	Tymczasowe pliki systemu Windows	5.02 MB
-	Dzienniki zdarzeń Windows	4.26 MB
	Tymczasowe pliki użytkowników	3.67 MB
ළු	Prefetch	1.88 MB
e	Tymczasowe pliki Edge	837 KB
e	Tymczasowe pliki Internet Explorer	606 KB
e	Historia Edge	304 KB
e	Cookies Edge	28 KB
	Zamknij	Wyczyść system

Wybranie "Wyczyść system" rozpoczyna usuwanie zbędnych plików – cała operacja może trochę potrwać zależenie 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:

m mks_	vir - czyszczenie systemu	- 🗆 X
m	ks_Vır	CZYSZCZENIE SYSTEMU
<b>P</b>	TEST01	Miejsce do odzyskania: 3.62 MB
-	Dzienniki zdarzeń Windows	3.57 MB
ඵ	Prefetch	43 KB
	Tymczasowe pliki systemu Windows	7 KB
	Zamknij	Wyczyść system

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", znajdujacy się w folderze c:\program files\mks vir\bin:

- I 🖓 📑 = I		Zarządzanie bin			– 🗆 ×
Plik Narzędzia główr	e Udostępnianie Widok	Narzędzia aplikacji			~ 🕐
← → ~ ↑ 📙 « D	ysk lokalny (C:) > Program Files >	→ mks_vir → bin →	・ つ Przeszuka	j: bin	
📥 Srubli dactan	Nazwa	Data modyfikacji	Тур	Rozmiar	^
J Szybki dostęp	TI fview	01.09.2020 11:15	Anlikacia	411 KB	
	dep01 dat	01.09.2020 11:15	Plik DAT	131 KB	
🕂 Pobrane 🛛 🖈	gen02 dat	01.09.2020 11:15	Plik DAT	372 KB	
🛗 Dokumenty 🛛 🖈	gentelaat	01.09.2020 11:15	Anlikacia	21 KB	
📰 Obrazy 🛛 🖈	he bin	01.09.2020 11:18	Plik BIN	3 KB	
Tan komputer	import root cert	01.09.2020 11:15	Anlikacia	100 KB	
	liberypto-1 1-x64.dll	01.09.2020 11:15	Rozszerzenie aplik	3 520 KB	
💣 Sieć	libeav32.dll	01.09.2020 11:15	Rozszerzenie aplik	2 095 KB	
	libssl-1 1-x64.dll	01.09.2020 11:15	Rozszerzenie aplik	805 KB	
	mfc120u.dll	01.09.2020 11:15	Rozszerzenie aplik	5 526 KB	
	mfcm120u.dll	01.09.2020 11:15	Rozszerzenie aplik	81 KB	
	m mks vir	01.09.2020 11:18	Aplikacja	473 KB	
	nks vira	01.09.2020 11:18	Aplikacja	411 KB	
	m mks_viraction	01.09.2020 11:18	Aplikacja	356 KB	
	限 mks_virdel	01.09.2020 11:15	Aplikacja	389 KB	
	m mks_vireol	01.09.2020 11:15	Aplikacja	268 KB	
	m mks_virlist	01.09.2020 11:15	Aplikacja	330 KB	
	m mks_virmenu	01.09.2020 11:19	Aplikacja	267 KB	
	m mks_virmf	01.09.2020 11:19	Aplikacja	4 196 KB	
	m mks_virmon	01.09.2020 11:19	Aplikacja	1 184 KB	
	m mks_virmsg	01.09.2020 11:15	Aplikacja	304 KB	
	m mks_virnotify	01.09.2020 11:15	Aplikacja	261 KB	
	🚾 mks_vir-podrecznik	01.09.2020 11:18	Microsoft Edge P	20 454 KB	
	mks_virproc	01.09.2020 11:15	Aplikacja	326 KB	
	📧 mks_virrd	01.09.2020 11:15	Aplikacja	123 KB	~
Elementy: 115 1 zaznac	zony element. 410 KB				800

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):

🖓 📙 🖛		Zarządzanie bin			- 0
Plik Narzędzia głów	ne Udostępnianie Widok Na	arzędzia aplikacji			~
÷ → • ↑ 📙 « ⊑	Jysk lokalny (C:) → Program Files → mks	s_vir → bin v	ව , Przeszuka	aj: bin	
📥 Szubki dostop	Nazwa	Data modyfikacji	Тур	Rozmiar	
🗶 szybki dőstép	mks virmf	01.09.2020 11:19	Anlikacia	4 196 KB	
Pulpit x	mks virmon	01.09.2020 11:19	Aplikacia	1 184 KB	
+ Pobrane 🕺	mks virmsa	01.09.2020 11:15	Aplikacia	304 KB	
🗄 Dokumenty 🛛 🖈	mks virnotify	01.09.2020 11:15	Aplikacia	261 KB	
📰 Obrazy 🛛 🚿	mks vir-podrecznik	01.09.2020 11:18	Microsoft Edge P	20 454 KB	
Ten komputer	mks virproc	01.09.2020 11:15	Aplikacia	326 KB	
	R mks virrd	01.09.2020 11:15	Aplikacia	123 KB	
💣 Sieć	m mks virrep	01.09.2020 11:15	Aplikacja	262 KB	
	m mks virsd	01.09.2020 11:15	Aplikacja	323 KB	
	m mks_virsend	01.09.2020 11:19	Aplikacja	336 KB	
	m mks_virsetup	01.09.2020 11:15	Aplikacja	346 KB	
	mks_virsupport-idcxxmp3tb	01.09.2020 11:15	Aplikacja	9 954 KB	
	m mks_virsv	01.09.2020 11:19	Aplikacja	4 107 KB	
	m mks_virupdate	01.09.2020 11:19	Aplikacja	4 278 KB	
	m mks_virupdate_executor	01.09.2020 11:24	Aplikacja	4 278 KB	
	mks_virusb	01.09.2020 11:15	Aplikacja	643 KB	
	mks_virwrap.dll	01.09.2020 11:19	Rozszerzenie aplik	2 810 KB	
	motor.dll	01.09.2020 11:15	Rozszerzenie aplik	201 KB	
	m msbe	01.09.2020 11:15	Aplikacja	317 KB	
	msvcp120.dll	01.09.2020 11:15	Rozszerzenie aplik	640 KB	
	msvcr120.dll	01.09.2020 11:15	Rozszerzenie aplik	937 KB	
	netscan2.dll	01.09.2020 11:19	Rozszerzenie aplik	232 KB	
	nfapi.dll	01.09.2020 11:15	Rozszerzenie aplik	200 KB	
	📧 nfregdrv	01.09.2020 11:15	Aplikacja	87 KB	
	📄 noeol.bin	01.09.2020 11:15	Plik BIN	1 KB	
lementy: 115   1 zaznac	zony element. 4,17 MB				

Elementy: 115 1 zaznaczony element. 4,17 MB

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:

Przeglądanie w poszukiwaniu folderu	×				
Wybierz folder do skanowania					
> 🛄 Pulpit	^				
> 📑 Wideo					
🗸 🏪 Dysk lokalny (C:)					
> 📙 Pliki programów (x86)					
> Program Files					
> ProgramData					
SAMPLES					
> Użytkownicy					
> 📙 Windows					
Dvsk lokalnv (D:)	~				
Eolder: SAMPLES					
Utwórz nowy folder OK Anuluj					

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

m mks_vir (tryb awaryjny)		- 🗆	×
mke vir	TF	RYB AWA	RYJNY
C:\SAMPLES\0ced9319e7562bf360b08ba7a6c22dcf9daf54	f1.exe.vir		18
		Sto	ор
Ścieżka	I	nfekcja	^
C:\SAMPLES\090083cfa98d90263f00054077e5611c	Win32.S	ality.OG	
☑ C:\SAMPLES\0934bf356504b8d2e9a5654d24ae67e8	Win32.S	ality.OG	
C:\SAMPLES\0937f1647a9eeebd52de84c5ecbe9b9da	Win32.S	ality.OG	
C:\SAMPLES\0978c171c82a49f723aec94c9d514c988	Win32.S	ality.OG	
✓ C:\SAMPLES\09e17c1339bf4db5d6a81a76fd3061f90	Win32.S	ality.OG	
C:\SAMPLES\09f99e8566412afab038e23ea5763d1eb	Win32.S	ality.2.0	E
☑ C:\SAMPLES\0a17141e5f5e1653b2f5118254645094	Win32.S	ality.OG	
ColCAMPLEC\052d10677b0140407bfc6c550b5022C2	Wienn C	Site 2 O	> `

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.

mks_vir (tryb awaryjny)		_		Х
mks_Vır		TRYB	AWAR	YNCY
Skanuj Mój Komputer	Skanuj	wybrany fold	er	
Ścieżka		Infek	cja	^
C:\SAMPLES\1811281e81d893015d72	705392197a5	Win32.Sality	.0G	
C:\SAMPLES\18ac7215c83497595c27a	ac563cc67a7f	Win32.Sality	.0G	- 14
C:\SAMPLES\1926738aa8b186dbbdb3	67da44c7c718	Win32.Sality	.0G	
C:\SAMPLES\196e63c486a79be422464	4dc651769720	Win32.Sality	.2.OE	
C:\SAMPLES\199ff1017d83a0ec6943d	253ed6c0249c	Win32.Sality	.2.0E	
C:\SAMPLES\19ae45d3db2256895bd5	8d86cb4db32c	Win32.Sality	.0G	
C:\SAMPLES\19ce34de1c922f5949fbaa	94a1ffbf732b	Win32.Sality	.OG	
C.\CAMPLEC\1040212200007a0a0f0a0	0cofF0f0c10b	Wienn Calify		、 <sup>×</sup>
• Usuń zagrożenia Skasuj	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 **?**.

-			_	~
m mks_vir administrator		-		×
mke	vir 😞			
iiika	<b></b>			
Logowa	nie do serwera			
	127.0.01			
Adres se	wera: 127.0.0.1			
Port:	4000			
Użytkow	admin			
Hasto				
husio.				
	Zalogui			

Jeśli serwer jest dostępny ikona ma kolor zielony 穼:

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):

mks_vir administrator			-	×
mk	s Vu	. 😞 🗖		
		4500 : Błąd 4501 : Błąd		
Logov	wanie do	serwera 4502 : Błąd 4503 : Błąd		
Adres	serwera:	127.0.0.1		
Port:		4500		
Użytko	wnik:	admin		
Hasło:				
		Zaloguj		

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

m mks_vir administrator	a Repozytori	idmin@127.0.0.1 12/0/4000 ium: 2024.05.29 09:03:21	- □ × Q <b>≟ ≎ Ø</b>					
A Zarządzane stacje     STACJE     STACJE     STACJA1     STACJA2     STACJA3     STACJA3     SSTACJA4     SERWER *	Zarządzane stacje (grupa)       grupa     ustawienia       O     Stacje w grupie są bezpie       W grupie są stacje z ocze       Podstawowe informacje o gru	ty oprogramowanie czne kującymi aktualizacjami Wi pie	podsumowanie					
	Liczba stacji w grupie: 5 Zakres wersji baz: 2024-05-29 09:03:21 Zakres abonamentów: 217 Uprawnienia: admin 🕼							
	🛃 Aktualizacja	Wyłącz stacje	Menadżer procesów					
	Skanowanie szybkie	Włącz stacje	Czyszczenie systemów					
	<b>Q</b> Skanowanie pełne	🗯 Restartuj stacje	Wyślij władomość					
	Wyczyść SafeStorage	Zablokuj stacje	Uruchom proces					
	Wyczyść kwarantannę		Podgląd pulpitów (*)					
	(*) Dowledz się więcej o możliwości d	odatkowej konfiguracji podgląd	tu pulpitów					

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  ${\bf Q}$  zmieni się w ikonę  ${\bf X}$  – 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
- O dostęp do podręcznika mks\_vir

#### Podstawowe informacje o grupie:

m mks_vir administrator			- 0	×
mks_Vır	Repozyto	admin@127.0.0.1 23/0/4000 rium: 2024.05.29 09:03:21	Q 🕹 🌣 🖨	9
Zarządzane stacje	STACJE (grupa) ustawienia rapo Stacje w grupie są bezpł W grupie są stacje z ocz Podstawowe informacje o gr Liczba stacji w grupie: 4 Zakres wersji baz: 2024 Zakres abonamentów: 217 Uprawnienia: admin	rty oprogramowanie eczne ekującymi aktualizacjami Wi uple -05-29 09:03:21	podsumowanie Indows	
	Akcje			
	📩 Aktualizacja	Wyłącz stacje	Menadżer procesów	
	🖌 Skanowanie szybkie	Włącz stacje	Czyszczenie systemów	
	Q Skanowanie pełne	C Restartuj stacje	Wyślij wiadomość	
	Wyczyść SafeStorage	Zablokuj stacje	Uruchom proces	
	Wyczyść kwarantannę		Podgląd pulpitów (*)	
	(*) Dowledz się więcej o możliwości	dodatkowej konfiguracji podgląd	lu 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 **Z** 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):

mks_vir administrator				-		×
					(	3
Stacja Miejsce do od STACJA1	dzyskania 721.1 MB	۲				
STACJA2 6	62.76 MB	۲				
STACJAS 6	553.51 MB	۲				
			Uruchom czyszczenie syst	temóv	v	

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

mks_vir administrator			_		×
mks_Vır	admin@127.0.0.1 22/0/4000 Repozytorium: 2024.05.29 09:03:21	Q	*	Ф	0
<ul> <li>A Zarządzane stacje</li> <li>A STACJE</li> </ul>	STACJE (grupa)				
STACJA1 STACJA2 STACJA3 STACJA4	grupa ustawlenia raporty oprogramowanie podsumowanie				
SERWER *	Uruchomienie procesu w STACJE				
	Proces do uruchomienia:				
	Parametry:				
			ŚW		
	Uruchom proces z wysokimi uprawnieniami		IIIOW		
	Anuluj Uruchom		(*)		
	(*) Dowledz się więcej o możliwości dodatkowej konfiguracji podglądu pulptów		,		

gdzie:

- Proces do uruchomienia tu podajemy nazwę pliku do uruchomienia, jeśli jest to konieczne razem ze ścieżką do 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 uprawnienami zalogowanego użytkownika

 Podgląd pulpitów – umożliwia wyświetlenie miniaturek 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:

m mks_vir administrator	admin@127.0.0.1 21/0/4000 Q 📩 🌣 🚱 Repozytorium: 2024.05.29 09:03:21
Zarządzane stacje	STACJA1 Etster Windows 10 Pro stacja ustawienia raporty oprogramowanie Stacja jest bezpieczna Podstawowe informacje o stacji
	Nazwa stacji:         TESTO1 [09cd1307-6e1d-a880-31142113610f]           Adres:         10.0.0101 [309c2341e24d]           Procesor:         1% intel(R) Core(TM) I3-7100 CPU @ 3.90GHz           Pamięć:         55% 3987MB           Dyski:         C 118GB 95 GB 24 931 GB 910 GB           Mejsce do odzyskania:         721.1 MB           Oczekujące aktualizacje:         2           Możliwy problem z dyskami:         Kliknij, żeby sprawdzlć.           Pakiet mks_vir         Kliknij, żeby sprawdzlć.
	Numer licencji:         TESTY-7898-BA94-A202-2011-0B0C-1087-D108-7F1E-10K1-G1H1-Z5           Licencja:         217           Wersja bazy:         2024-05-29 09:03:21           Dodatkowe informacje:         Akcje
	▲ Aktualizacja       ① Wyłącz stację       ➡ Menadżer procesów         ✓ Skanowanie szybkie       ① Włącz stację       □ Zdalny pulpit (RDP)         Q Skanowanie pełne       ② Restartuj stację       ● Podgląd pulpitu (*)         Im Wyczyść SafeStorage       Im Audyt systemu       ● Wyślij władomość         ★ Kwarantanna       Im Audyt systemu       ● Uruchom proces         ✓ Stan systemu       ✓       Vruchom proces

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):

mks_vir administrator		- 🗆 ×
mks_Vır	admin@127.0.0.1 22/0/4000 Repozytorium: 2024.05.29 09:03:21	Q 🛣 🏶 😧
<ul> <li>Zarządzane stacje</li> <li>STACJE</li> </ul>	STACJA1 Lester Windows 10	
🖵 STACJA1	stacja ustawienia raporty oprogramowanie	
🖵 STACJA3 🖵 STACJA4	Stacja jest bezpieczna	
SERWER ★	Podstawowe informacje o stacji	
	Czyszczenie systemu	
	Czy chcesz usunąć zbędne pliki na wybranej stacji?	
		-Z5
	Nie	ak
L	🛃 Aktualizacja 🕖 Wyłącz stację 📰	Menadzer procesów
	🖌 Skanowanie szybkie 💿 Włącz stację 📃	Zdalny pulpit (RDP)
	🔾 Skanowanie pełne 🛛 🔁 Restartuj stację 🌑	Podgląd pulpitu (*)
	🛅 Wyczyść <i>SafeStorage</i> 🔒 Zablokuj stację 🗩	Wyślij wiadomość
	🛧 Kwarantanna 📊 Audyt systemu 🌍	Uruchom proces
	Market Stan systemu	

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 aktualizację"** 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:

m mks_vir - stan systemu	-		×
	Ţ	TEST	101
Wydajność systemu (procesor/pamięć/starty systemu)			
ostatnia godzina ostatnie 24 godziny ostatnie 7 dni ostatnie 30 dni			
Procesor 7%			
100%			
0%			
III Pamlęć 49%			
100%			
O Starty systemu 1			

– Dyski:

	systemu					-	
	Q					Ţ	TEST1
yski							
Lista dyskó	w fizycznych						
Model		Serial	Rozmiar	Partycje			
ST1000D	M010-2EP102	Z9AP4S4Z	931.5 GB	Z:			
ADATA S	SU800	2H4320092706	119.2 GB	C:			
Status dysk	ków fizycznych ADATA SU8	(S.M.A.R.T.) 00		C:			
Status dysk 🕑 Status	ków fizycznych ADATA SU8 Parameter	(S.M.A.R.T.) 00	Curr	C: ent Worst	Threshold	Data	
Status dysk Status Status	ków fizycznych ADATA SU8 Parameter Raw read erro	(S.M.A.R.T.) 00 r rate (1)	Curr 100	C: ent Worst 100	Threshold 0	Data 0	
Status dysk Status Status	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se	(S.M.A.R.T.) 00 r rate (1) ector count (5)	Curr 100 100	C: ent Worst 100 100	Threshold O O	Data O 1	
Status dysk Status Status A S	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou	(S.M.A.R.T.) OO Ir rate (1) Ector count (5) rs count (9)	Curr 100 100 100	C: ent Worst 100 100 100	Threshold O O O	Data 0 1 3837	
Status dysk Status A Status	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle co	(S.M.A.R.T.) OO rr rate (1) ector count (5) rs count (9) ount (12)	Curr 100 100 100 100	C: ent Worst 100 100 100 100	Threshold O O O O O	Data 0 1 3837 1795	-
Status dysk Status C A C C C C C C C C	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle co Power-off retr	(S.M.A.R.T.) OO Ir rate (1) ector count (5) rs count (9) ount (12) act count (192)	Curr 100 100 100 100 100	C: Worst 100 100 100 100 100	Threshold O O O O O O O O	Data 0 1 3837 1795 48	
Status dysł Status Status C C C C C C C	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle co Power-off retr HDD temperat	(S.M.A.R.T.) 00 r rate (1) ector count (5) rs count (9) ount (12) act count (192) ture (194)	Curr 100 100 100 100 100 100	C: 900 100 100 100 100 100 100 100	Threshold           0	Data 0 1 3837 1795 48 40	

– Przeglądarki:

👖 mks_vir - stan systemu			
🖿 🗁 <u>ଓ</u>			
Przeglądarki			
Strony z ustawieniami powia	adomień	(2025.06.2	4 10:36:
strony z ustawienianii powie	aonnen	(2025.00.2	4 10.50.
Wszystkie Dozwolone	Zablok	owane Do	omyślne
			-
<b>— —</b> 1			
💽 Edge			
Strona	Profil	Użytkownik	Status
https://tvn24.pl:443,*	Default	tester	Allow
https://www.gazeta.pl:443,*	Default	tester	Deny
https://www.interia.pl:443,*	Default	tester	Deny
https://www.onet.pl:443,*	Default	tester	Allow
https://www.wp.pl:443,*	Default	tester	Deny
Intip3.//www.wp.pi.443,	Delduit	tester	Deny

 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

	admin@127.0.0.1 22/0/4000 Repozytorium: 2024.05.29 09:03:21	Q	*	\$ ×
A Zarządzane stacje     A Ś STACJE     G STACJA1     G STACJA2     G STACJA3     G STACJA3     G STACJA4     Aki	Zarządzane stacje (grupa) pa ustawienia raporty oprogramowanie podsumowanie rywność modułów ochronnych			
SERWER *	Ochrona plików       Ochrona poczty         Ochrona przeglądarki       Ochrona przeglądarki         Zapora sieciowa (firewali)       Ochrona odzicieliska         Kontrola urządzeń WSB       Ochrona plikacji         Kontrola urządzeń multimedialnych       Ochrona rejestru         Ochrona RoundKick EDR       Ochrona RoundKick EDR         Dostęp do Internetu       Ochrona rejestru         wienia       Waż szczegółowe ustawienia pakietu mks_vir         mer licencji       Zmieri	ί numer	licencii	

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 (fire-wall)** – 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:

mks_vir administrator						-		×
mks_Vır	Repozy	admir 22/ torium: 1	n@127.0.0.1 ′0/4000 2024.05.29 10:09:33		Q	*	\$	Ø
Zarządzane stacje	arządzane stacje							
- STACJA1 - STACJA2 grupa	ustawienia ra	porty	oprogramowanie	podsumowanie				
STACJA3	ystyki grupy są wyl	iczane n	a podstawie raportów	o wykrytych infekcjac	h z ostatni	ch 30 dn	i.	
			_					
Eks	portuj wszystkie rapoi	ty grupy	do pliku CSV					
TOP 10	wykrytych infekcji	w grupie	e					
	Win32.Sality.OG	3						
EICAR-Te	est-File (not a virus)	2			_			
	Trojan.A	1						
Tr	ojan.Mikey.D23070	1						
Win32		1						
v	Vin32.Virtob.Gen.12	1						
, , , , , , , , , , , , , , , , , , ,	Win32.Virtob.3.Gen	1						
TOP 10 s	stacji z wykrytymi	infekcjai	mi w grupie					
STACJA	1 5							
STACJA2	2 5							

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:

m mks_vir administrator			- 🗆 X
mks_Vır	adn 2 Repozytorium	nin@127.0.0.1 5/0/4000 n: 2024.05.29 10:09:33	Q 🕹 🌣 🛛
Zarządzane stacje     STACJE     STACJA1     STACJA2	stacja ustawienia raporty	tester • Windows 10 Pro oprogramowanie	
→ ♀ STACJA3 → ♀ STACJA4 → ♀ SERWER ★	Raporty z dnia: 2025-03-17 🔽	Pokaż historię przeglądanych stron	Pokaż aktywność sieciową
	2025-03-17 10:11:57 2025-03-17 10:10:08 2025-03-17 10:07:31 2025-03-17 07:42:05 2025-03-17 07:42:05 2025-03-17 01:41:19	Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu	3803           4           4           4           4           4
			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*":

mks_vir administrator			- 🗆 ×
mks_Vır	Repozyt	admin@127.0.0.1 25/0/4000 orium: 2024.05.29 10:09:33	C ∓ 🌣 🖯
- 🕷 Zarządzane stacje	STACJA1 (stacja)	Lester Vindows 10	Pro
🖵 STACJA1 🖵 STACJA2	stacja ustawienia rap	orty oprogramowanie	
STACJA3		Rapo	rty o infekcjach z ostatnich 30 dni
SERWER X	Data	Zdarzenie	Status
	2025 02 12 12:20:45	Skapowapie felderów i plików	Infolgio
	2025-03-13 12:38:45	Skanowanie folderów i plików	Intekcja
	2025-03-13 12:38:08	Monitor wykrył szkodiwy obiekt	Infekcja
	2025-03-13 12:33:32	Monitor wykrył szkodiwy obiekt	Infekcja
	2025-03-13 12:33:20	Monitor wykrył szkodiwy obiekt	Infokcia
	2025-03-13 12:33:05	Monitor wykrył szkodliwy obiekt	Infekcja
	2025-03-13 12:32:47	Monitor wykrył szkodliwy obiekt	Infekcja
	2025-03-13 12:32:47	Monitor wykrył szkodliwy obiekt	Infekcja
	2025-03-13 12:30:16	Monitor wykrył szkodliwy obiekt	Infekcia
	2025-03-13 12:50:10	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	Infekcia
	2025-03-11 08:24:57	Monitor wykrył szkodliwy obiekt	Infekcia
	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

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

m mks_vir - histori		-		×	
Historia przeglą	danych stron z dnia: 2020.12.17	🔽 Pokaż	wszys	stkie ac	iresy
08:23:01	tvn24.pl				
08:22:54	www.gazeta.pl				
08:22:54	gazeta.pl				
08:22:53	pogoda.wpcdn.pl				
08:22:51	fonts.googleapis.com				
08:22:43	v.wpimg.pl				
08:22:43	fonts.wpcdn.pl				
08:22:42	www.wp.pl				
08:22:42	wp.pl				
08:22:36	www.onet.pl				
08:22:35	onet.pl				
08:22:33	login.wikimedia.org				
08:22:33	meta.wikimedia.org				
08:22:33	en.wikipedia.org				
08:22:30	upload.wikimedia.org				
08:22:30	consent.youtube.com				
08:22:30	pl.wikipedia.org				
08:22:29	consent.google.pl				
08:22:28	play.google.com				
08:22:25	ogs.google.com				
08:22:25	apis.google.com				
08:22:18	consent.google.com				
08:22:17	www.google.com				
08:22:17	privacyportal.onetrust.com				
08:22:14	r.bing.com				
08:22:14	www.bing.com				
08:22:13	arc.msn.com				
08:22:11	assets.msn.com				
08:22:11	config.edge.skype.com				

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:

mks_vir - aktywność sieciowa						-		Х
Aktywność sieciowa z dnia	: 2025.04.17		Dane lokalizacyjne	dostar	cza ᠙ IF	Pinfo		
Filtry	08:25:44 msedg	e.exe	18.66.233.111	443	-		Poland	*
V Przepuszczone 285	08:25:44 msedg	e.exe	18.66.233.111	443	-		Poland	
Zablokowane 🛛 🛛	08:25:44 msedg	e.exe	18.66.233.111	443	-		Poland	
	08:25:44 msedg	e.exe	13.227.146.106	443	-		Poland	
🗹 Przychodzące 🗧 🌼	08:25:44 msedg	e.exe	23.88.75.103	443	_		Germany	/
Vychodzące 🗲 285	08:25:43 msedg	e.exe	151.101.1.229	443			United	St
VIP v4 285	08:25:43 msedg	e.exe	54.38.136.25	443	-		Poland	
	08:25:43 msedg	e.exe	13.227.146.106	443	-		Poland	
	08:25:43 msedg	e.exe	34.36.214.49	443			United	St
Aplikacje	08:25:43 msedg	e.exe	84.17.61.32	443			Czechia	3
mousocoreworker.exe	08:25:43 msedg	e.exe	2.20.32.236	443	-		Poland	
🗸 msedge.exe	08:25:43 msedg	e.exe	13.227.146.71	443	-		Poland	
< msedgewebview2.exe	08:25:43 msedg	e.exe	13.227.146.71	443	-		Poland	
🗸 searchapp.exe	08:25:43 msedg	e.exe	13.227.146.8	443	-		Poland	
✓ smartscreen.exe	08:25:43 msedg	e.exe	216.58.215.78	443	-		Poland	
svchost.exe	08:25:43 msedg	e.exe	20.79.107.10	443	-		Germany	/
systemsettings.exe	08:25:43 msedg	e.exe	13.227.146.106	443	-		Poland	
	08:25:43 msedg	e.exe	178.239.128.20	443	-		Poland	
	08:25:42 msedg	e.exe	13.227.146.31	443	-		Poland	
	08:25:42 msedg	e.exe	13.248.170.130	443			United	St
	08:25:42 msedg	e.exe	75.2.119.157	443	922		United	St
	08:25:42 msedg	e.exe	15.197.153.132	443			United	St≖
	-			)				•

- Filtry pozwala na filtrację aktywności:
  - dla połączeń przepuszczonych lub zablokowanych
  - dla połączeń przychodzących ( $\leftarrow$ ) lub wychodzących ( $\rightarrow$ )
  - 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:

mks_vir administrator			-	
mks_Vır	admin@127.0.0.1 20/0/4000 Repozytorium: 2024.05.29 10:09:33		Q 🛃 I	¢ 0
A Zarządzane stacje A STAC IE	STACJA4 stester	Windows 11 Pro		
STACJA1 STACJA2 STACJA3	stacja ustawienia raporty oprogramowanie			
STACJA4	Oprogramowanie zainstalowane w systemie			
📖 🖵 SERWER 🖈	☑ Ukryj aktualizacje systemu Windows	Filtr:		
	Aplikacja Microsoft Edge Update Microsoft Update Health Tools mks_vir Środowisko uruchomieniowe Microsoft Edge WebView2	Producent Microsoft Corporation Microsoft Corporation Arcabit/mks_vir Microsoft Corporation	Wersja 125.0.2535.67 1.3.187.39 5.72.0.0 125.0.2535.67	

#### **Podsumowanie:**

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

	R	adı 2 epozytoriur	min@127.0 22/0/4000 m: 2024.05	.0.1 ) 5.29 10:0	9:33		C	λ 🛣	<b>\$</b> (	8
grupa	ACJE <sup>pa)</sup> ustawienia	raporty	oproç	gramow	anle pod	sumowani	e			
EKS	portuj podsum	iowanie grup	y do pliku C:	5V		dok podst Wersla	awowy	Oczekulace	%	
STACJA1	10.0.0.101	Windows 10 Pro 6.2 X64	Intel(R) Core (TM) I3- 7100 CPU @ 3.90GHz Intel(R)	3987	tester	2024- 05-29 09:03:21	Abonament 217	aktualizacje 2	Pamlęć 55%	Pr 19
STACJA2	10.0.0.102	Windows 7 Ultimate 6.1 X64 SP 1.0	Core (TM) I3- 4130 CPU @ 3.40GHz Intel(R)	3983	tester	2024- 05-29 09:03:21	217	0	28%	0'
STACJA3	10.0.0.103	Windows 8.1 Pro 6.2 X86	Core (TM) I3 CPU 540 @ 3.07GHz Intel(R)	3447	tester	2024- 05-29 09:03:21	217	1	26%	0'
STACJA4	10.0.0.104	Windows 11 Pro 6.2 X64	Core (TM) I3- 9100 CPU @ 3.60GHz	16246	tester	2024- 05-29 09:03:21	217	2	16%	0!
	Grupa Grupa Eks Nazwa STACJA1 STACJA2 STACJA3 STACJA4	Control Contro Control Control Control Control Control Control Control Control Co	Rep22violation rep22violation grupa ustawienia raporty Exsportuj podsumowanie grup Nazwa IP System STACJA1 10.0.0.101 Windows STACJA2 10.0.0.102 Windows STACJA2 10.0.0.103 Windows STACJA3 10.0.0.103 Windows STACJA3 10.0.0.103 Windows STACJA4 10.0.0.104 Windows STACJA5 10.0.0.0.104 Windows STACJA5 10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.	STACJA2 10.0.0102 GIVEN CM 10.0.0103 GIVEN CM 10.0.0010 GIVEN CM 10.0.	STACJA2 10.0.0101 Windows CFU a 300GHz 1010 1000 1000 1000 1000 1000 1000 10	Nackada       Stacle         grupa       ustawlenia       raporty       oprogramowanie       pods         Response       Process       Panityc       Ustawlenia       constraints         Nazwa       IP       System       Process       Panityc       Ustawlenia         Nazwa       IP       System       Process       Panityc       Ustawlenia         STACJA1       10.0.0.101       Windows       Crup a Crup a 3.900Hz       3.987       tester         STACJA2       10.0.0.102       Windows       Crup a Crup a 3.900Hz       3.983       tester         STACJA2       10.0.0.102       Windows       Crup a Crup a 3.000Hz       3.947       tester         STACJA3       10.0.0.104       Windows       Crup a Crup a 3.000Hz       3.447       tester         STACJA4       10.0.0.104       Windows       Crup a Crup a 3.000Hz       16246       tester	STACJE (STRP3)         Stack           Srupa         ustawienia         raporty         oprogramowanie         podsumowanie           Eksportul podsumowanie grupy do pilku CSV <ul></ul>	STACJA       grupa       ustawlenia       raporty       oprogramowanie       podsumowanie         Grupa         Ustawlenia       raporty       oprogramowanie       podsumowanie         Colspan="4">Colspan="4">Widok podsumowanie         Core       Official CSV         Nintel(R)         STACJA1       10.0.0.101       Windows         Core       Core       Core         STACJA1       10.0.0.101       Windows         Vindows         Core       Core       Core         STACJA2       10.0.0.101       Windows         Vindows       Core       Core         STACJA2       10.0.0.102       Windows         Vindows       Core         Core       Core       Core         STACJA2       10.0.0.102       Windows       Core         Vindows       Core       Core       Core       Core <th>STACJE       grupa       ustawlenia       raporty       oprogramowanic       podsumowanic         Exportul podsumowanie grupy do piku CSV</th> <th>STACJE         Constraint         Constraint&lt;</th>	STACJE       grupa       ustawlenia       raporty       oprogramowanic       podsumowanic         Exportul podsumowanie grupy do piku CSV	STACJE         Constraint         Constraint<

Możliwe jest też zapisanie podsumowania grupy do pliku tekstowego w formacie CSV (potem można taki plik przetwarzać np. w Microsoft Excel, LibreOffice Calc itp.) za pomocą przycisku "*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

### $\textbf{Ochrona} \rightarrow \textbf{Ochrona plików:}$

m	mks_vir administrator		-		×
		admin@127.0.0.1			
l	Zarządzane sta (grupa)	acje	Ustav	vienia	
L	ochrona	U 🏛 🖂 % A 🏎 🖸 端 f 🚍			
		✓ Aktywuj ochronę antywirusową Akcje			I
	kontrola rodzicielska	Po znalezieniu zagrożenia: Usuń zagrożenie 💟 Włącz powiadomienia dla akcji automatycznych			
	aktualizacja	Poziom heurystyki			I
	🔶 ogólne	Ustawienia dodatkowe			I
	android	Włącz skanowanie archiwów Włącz skanowanie zasobów sieciowych Skanuj tylko pliki nosiciele Biokuj autostart na nościłkach USB			I
	zarządzanie	Optymalizuj dostęp do zasobów chmurowych Optymalizuj dostęp do przeglądarek internetowych			I
					I
		🖅 Grupa nie ma zdefiniowanego własnego numeru licencji – Zmie	eń numer licencii		

Aktywuj ochronę antywirusową – opcja aktywuje najważniejszy moduł ochronny pakietu mks\_vir

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

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

#### Ustawienia dodatkowe:

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

#### $\textbf{Ochrona} \rightarrow \textbf{SafeStorage:}$

*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.



m	mks_vir administrator		-		×
		admin@127.0.0.1		_	
	Zarządzane s (grupa)	- L	Istawie	enia	
	ochrona	U 🏛 🖂 % 🗛 🤟 🖾 🧳 🗁			
I	<b>Q</b> skanowanie	Wiącz aktywną ochronę danych SafeStorage     □ Chroń również pilki na zasobach sieciowych			l
l	kontrola rodzicielska	Ta opcja powinna być włączona tylko wtedy, gdy przechowujesz pliki na dyskach sieciowych i cho chronić w ramach lokalnego mechanizmu SafeStorage.	esz je		
l	📩 aktualizacja	Automatycznie wybieraj foldery chronione przez <i>SafeStorage</i>			I
l	🗙 ogólne				I
l	in android				I
I	Zarządzanie				l
I					I
					Ļ
		Grupa nie ma zdefiniowanego własnego numeru licencji Zmień nymerice	ncii		

**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

#### $\textbf{Ochrona} \rightarrow \textbf{Ochrona poczty:}$

m	mks_vir admi	inistrator		-		$\times$
		_	admin@127.0.0.1		_	
		arządzane st <sup>upa)</sup>	acje	Ustawi	ienia	
4	•	chrona	V 🏛 🖂 % 🗛 🤟 🙆 🐝 १ 🚍			l
	Q sk	anowanie	Aktywuj ochronę poczty Ustawienia zaawansowane			I
		ontrola odzicielska	Pozlom heurystyki Normalny			
	📩 ak	ctualizacja	Akcje Po znalezieniu zagrożenia: Zabezpiecz zainfekowaną zawartość			I
		góine	Antyspam			ł
	뼦 <sup>ar</sup>	ndrold	Aktywuj moduł antyspamowy Lista reguł modułu antyspamowego Znacznik spamu: ***SPAM***			I
	in the second se	arządzanie				l
			₽ ★			
k				concil		
			E X	icencii		

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

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



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

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

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

Antyspam – moduł do znakowania wiadomości-śmieci

#### $\textbf{Ochrona} \rightarrow \textbf{Ochrona} \text{ przeglądarki:}$

mks_vir administrator		- 0	] >
Zarządzane s (grupa)	admin@127.0.0.1	Ustawie	nia
<b>O</b> ochrona	U 🏛 🖂 💁 🗛 🍜 🖸 端 1 🚍		
	⊠ Aktywuj ochronę przeglądarki Poziom heurystyki		
kontrola rodzicielska	Normalny  Vstawienia biokowania		
📩 aktualizacja	Blokuj pobleranie nlepodpisanych plików wykonywalnych     Blokuj transmisje strumieniowe (audio/video)     Blokuj popularne serwisy reklamowe		
🗙 ogólne	Ustawienia dodatkowe		
android			
zarządzanie			
	Grupa nie ma zdefiniowanego własnego numeru licencji Zmień nymer	licencii	

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

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

#### Ustawienia blokowania

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

#### Ustawienia dodatkowe

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

#### $\textbf{Ochrona} \rightarrow \textbf{Zapora sieciowa (firewall):}$

m	mks_vir administrator		- 0	×
	_	admin@127.0.0.1		
l	Zarządzane st (grupa)	tacje Ug	stawienia	
	ochrona	V 🏛 🖂 % 🛕 🤝 🖸 🐝 1⁄ 🚍		
	<b>Q</b> skanowanie	Aktywuj zaporę sieciową  Sostosuj aktywność zapory Windows do zapory mks_vir  Czepowszczal polaczenia wychodzace		
	kontrola rodzicielska	<ul> <li>✓ Przepuszczaj połączenia w sieci lokalnej</li> <li>✓ Blokuj aktywność sieciową skryptów</li> <li>□ Blokuj połączenia IPv6</li> </ul>		Î
	📩 aktualizacja	Reguły zapory sieciowej Definicje sieci lokalnych		I
	🔶 ogólne	Podaj definicje sieci lokalnych oddzielając je spacjami, np.: 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 FEU FCOO::/7	80::/10	
	android	192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 169.254.0.0/16 FE80:		I
	2arządzanie			
		E Grupa nie ma zdefiniowanego własnego numeru licencji Zmień numerlicen	cii	ĺ

Aktywuj zaporę sieciową – aktywuje moduł ochrony sieci

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

## $\textbf{Ochrona} \rightarrow \textbf{Kontrola} \text{ urządzeń USB:}$



Aktywuj kontrolę urządzeń USB – aktywuje moduł kontroli urządzeń USB

Ustawienia – umożliwia konfigurację modułu kontroli urządzeń USB

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

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

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

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

m	mks_vir a	administrator												-		×
1	**	Zarządzane s <sup>(grupa)</sup>														1
	U	ochrona	U	<b></b>		00			0	<b>Q</b> 0	4					
	Q			ktywuj k Lista r	controle eguł dla	urządze urząd	ní USB zeń US	В								-
	Ť		Gđ					Urządz	enie				Dostęp		•	
	*		Re												4	-
	*		N													
				Doda	ai urzadz	enie							7a	mknii	. I	
				Jour	-j-meque							_			2	
								B	×							

### Ochrona $\rightarrow$ Kontrola urządzeń multimedialnych:



**Aktywuj kontrolę urządzeń multimedialnych** – aktywuje moduł kontroli urządzeń multimedialnych

Ustawienia – umożliwia konfigurację modułu kontroli urządzeń multimedialnych

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

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

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

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



#### $Ochrona \rightarrow Kontrola aplikacji:$



Aktywuj kontrolę aplikacji – aktywuje moduł kontroli aplikacji

Ustawienia – umożliwia konfigurację modułu kontroli aplikacji

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

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

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

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

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



## $\textbf{Ochrona} \rightarrow \textbf{Ochrona} \ \textbf{RoundKick} \ \textbf{EDR:}$

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 natychmia-stowa 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 skanująch 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)

🔲 mis vis administratos		
···· mis_vir auministrator		- L X
	admin@127.0.0.1	
(grupa)	stacje	Ustawienia
<u></u>		
ochrona	◐ ፹	
	Chroń schowek systemowy w bezpiecznej przeglądarce	
skanowanie	✓ Utrzymuj okna bezpiecznej przeglądarki zawsze na wierzchu Wiesz ostrono cieci dla bezpiecznej przeglądarki.	
	Autócz ochronę sieci dla bezpiecznej przeglądaliki	~
kontrola rodzicielska		
Touzicieisku		
🚽 aktualizacja		
🔶 ogólne		
📥 android		
•		
zarządzanie		
	🖅 Grupa nie ma zdefiniowanego własnego numeru licencji Zmień num	ler licencii

## $\textbf{Ochrona} \rightarrow \textbf{Bezpieczna} \ \textbf{przeglądarka:}$

- 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 $\rightarrow$ Skanowanie pełne:

m	mks_vir a	administrator		-	$\square$ ×
			admin@127.0.0.1		_
	ю <b>:</b>	Zarządzane s <sup>(grupa)</sup>	tacje	Ustawi	enia
4	U	ochrona	skanowanie pełne skanowanie szybkie kwarantanna		
I	Q	skanowanie			-1
	Ŷ	kontrola rodzicielska	Po znalezieniu zagrozenia: <u>vic nie rob (tylko raport)</u> Poziom heurystyki		
	*	aktualizacja	Wysoki V Ustawienia dodatkowe		
	*	ogólne	☑ Włącz skanowanie archiwów ☑ Usuń piliki tymczasowe przed rozpoczęciem skanowania □ Spowolnij skanowanie, gdy użytkownik jest aktywny		- 1
	÷	android	O Harmonogram skanowania		- 1
		zarządzanie			- 1
					- 1
					- 1
			🖅 Grupa nie ma zdefiniowanego własnego numeru licencji	Zmień numer licencii	

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

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

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

#### Ustawienia dodatkowe:

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

## Skanowanie $\rightarrow$ Skanowanie szybkie:

т	mks_vir administrator		- 🗆 X
		admin@127.0.0.1	
	Zarządzane st	acje	Ustawienia
4	<b>O</b> ochrona	skanowanie pełne skanowanie szybkie kwarantanna	
I		Uruchom szybkie skanowanie przy starcie systemu Uruchom szybkie skanowanie po zalogowaniu użytkownika Uruchom szybkie skanowanie po aktualizacji Uruchom szybkie skanowanie powych pośpików USB	
	kontrola rodzicielska	Akcje	
	📩 aktualizacja	Po znalezieniu zagrożenia: Usuń zagrożenie 💌 Poziom heurystyki	
	🔶 ogólne	Normalny	
	android		
	zarządzanie 🔁		
		🖅 Grupa nie ma zdefiniowanego własnego numeru licencji	Zmień numer licencii

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

- przy starcie systemu
- po zalogowaniu użytkownika
- po aktualizacji programu mks\_vir
- po podłączeniu nośnika USB skanowana jest wtedy zawartość takiego nośnika

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

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

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

## Skanowanie $\rightarrow$ Kwarantanna:

т	mks_vir a	dministrator					- 0	×
l	:C:	Zarządzane s <sup>(grupa)</sup>	tacje	admin@127.	0.0.1		Ustawienia	
4	U	ochrona	skanowanie pełne	skanowanie szybkie	kwarantanna			Ţ
l	Q	skanowanie	□ Skanuj zawartość I ✓ Usuwaj z kwaranta	warantanny po aktualizacj nny pliki starsze niż 30 dni	ji pakietu			
	Ť	kontrola rodzicielska						1
	*	aktualizacja						I
	*	ogóine						I
	- <b>- - - - - - - - - -</b>	android						I
		zurządzunie						I
								I
					×			ł
ľ			See Grupa nie	ma zdefiniowanego wł	asnego numeru licencji	Zmień numer lice	encii	~

Automatyczne skanowanie i czyszczenie ze starych plików kwarantanny programu mks\_vir:

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

## Kontrola rodzicielska:

m	mks_vir a	administrator		-		×
	_		admin@127.0.0.1			
1	-0-	Zarządzane s (grupa)	stacje	Ustav	vienia	
4		ochrona	🗌 Aktywuj kontrolę rodzicielską			
			Tryb kontroli treści			
	Q	skanowanie	<ul> <li>Blokuj dostąp do wszystkich stron (z wyjątkami z listy reguł użytkownika)</li> <li>Blokuj dostęp do stron zgodnie z kategoriami (z wyjątkami z listy reguł użytkownika)</li> </ul>			L
			Pokaż listę kategorii			$\sim$
	Ĩ	kontrola rodzicielska	Pokaż listę reguł użytkownika			-82
			Pokaż listę użytkowników wykluczonych z kontroli rodzicielskiej			
	*	aktualizacja	⊠ Włącz bezpieczne wyszukiwanie ⊠ Blokuj pobieranie programów z Internetu			I
		ogólne	Harmonogram dostępu do sieci			
			Harmonogram dostępu do sieci			1
	<u> </u>	android				
	<b>9</b> -9	zarzadzania				
		Zarząuzanie				
			A Grupa nie ma zdefiniowanego własnego numeru licencji Zmień numer	icencii		

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":

m	mks_vir a	administrator		-		×
1						
		Zarządzane s (grupa)	stacje			
	U		Aktywuj kontrolę rodzicielską Trista kategorii kontroli rodzicielskiej			
	Q		Pornografia i seks		п	
	¥	kontrola rodzicielska	☑ Wulgaryzmy       ☑ Samobójstwo		1	
	*		☑ Sleci społecznościowe       ☑ Sleci społecznościowe       ☑ I Hazard			
	*		H. D Broń, pirotechnika		ł	
					1	I
					1	I
			Zamk	nii	. I	I
			Zallik		4	
			an Grupa nie ma zdefiniowanego własnego numeru licencji Zmiejinumerik	encii l		

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

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

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

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

## Aktualizacja:

m	mks_vir a	administrator		-		×
	-		admin@127.0.0.1			
I	-0-4 	Zarządzane s <sup>(grupa)</sup>	stacje	Ustaw	vienia	
	U	ochrona	☑ Aktualizuj automatycznie			
	Q	skanowanie	Serwer: Serwer zarządzający mks_vir			I
	Ŷ	kontrola rodzicielska	Opcje aktualizacji OHarmonogram aktualizacji			
	<b>.</b>	aktualizacja	Potwierdzaj aktualizację modułów programu Proxy			I
	*	ogólne	Užyj serwera proxy			I
	ŵ	android				I
		zarządzanie				I
						I
	_		🖅 Grupa nie ma zdefiniowanego własnego numeru licencji Zmień numerij	cencii	-	~

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

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

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

### Opcje aktualizacji:

Harmonogram aktualizacji – umożliwia określenie, kiedy ma być bezwzględnie wymuszana aktualizacja programu mks\_vir

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

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

## Ogólne:

т	mks_vir a	administrator	:	ĸ
			admin@127.0.0.1	
I	ю <b>:</b>	Zarządzane s <sup>(grupa)</sup>	tacje Ustawienia	
4	U	ochrona	O Ustawienia szczegółowe	
			Globalne wykluczenia ochrony	
	Q	skanowanie	Lista wykluczonych domen internetowych	
			Lista wykluczonych plików i folderów	~
	Ŷ	kontrola rodzicielska	C Lista wykluczonych procesów	L
			Porty i protokoły	
	<b>.</b>	aktualizacja	Tabela skanowanych i wykluczonych portów i protokołów	
			Folder danych	
	$\mathbf{x}$	ogólne	Folder, w którym są przechowywane potencjalnie duże ilości danych - kwarantanna, SafeStorage, kopie zanasowa szutrowane duski	
	<b></b>	android	☑ Korzystaj z domyślnego folderu danych pakietu mks_vir	
		zarządzanie		
	_		ET Grupa nie ma zdefiniowanego własnego numeru licencji Zmień numer licencji	1

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

m	mks_vir administrator		- 0	×
1	Zarządzane stacje			r.
	↓       ochrona       G         Q       skanowanie       G         Y       kontrola       G         rodzicielska       Pr         aktualizacja       G         Image: Space of the state of	Ustawienia szczegółowe Ustawienia szczegółowe  Aktywuj autoochronę pakietu mks_vir Kopiuj leczone pliki do kwarantanny Wiącz chortroje zajetości procesora Wiącz niskopoziomowe wykluczenia zapory Aktywuj ochronę w chmurze Okaż klasyczną ikonę mks_vir w zasobniku Czezwalaj na protokół GUIC Viącz akcelerację udostępniania szyfrowanych dysków Okaż konsolę szyfrowanych dysków po zalogowaniu Pokaż konsolę sirzeżenia o problemach z dyskami fizycznymi Ø Pokażuj ostrzeżenia o innych aplikacjach ochronnych Nie pokażuj monitów o zbliżającym się końcu abonamentu	u	
	Sarządzanie	Wyłącz komputer o godzinie:         Zabiokuj system po czasie nieaktywności (w minutach):         Zamknij		
		🖺 🗙		
				- V

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

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

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

- Nie skanuj połączeń lokalnych http wyłącza skanowanie protokołu HTTP dla połączeń realizowanych wewnątrz systemu operacyjnego (dla połączeń w adresacji 127.x.x.x)
- Wykrywaj aplikacje typu Asystent pobierania włącza wykrywanie tzw. Asystentów pobierania jako zagrożeń
- Pokaż konsolę szyfrowanych dysków po zalogowaniu włącza automatyczne wyświetlanie konsoli zarządzającej szyfrowanymi dyskami w programie mks\_vir po zalogowaniu użytkownika w systemie
- Włącz akcelerację udostępniania szyfrowanych dysków przyspiesza podłączanie szyfrowanych dysków do systemowych mechanizmów obsługi systemów plików
- Pokaż konsolę administracyjną w menu mks\_vir w zasobniku włącza dostęp do konsoli administracyjnej programu mks\_vir administrator w menu podręcznym ikony mks\_vir w zasobniku systemowym
- Włącz niskopoziomowe wykluczenia zapory włącza obsługę wykluczeń plików lub folderów zdefiniowanych w sekcji *Lista wykluczonych plików i folderów*, w zaporze programu mks\_vir
- Włącz akcelerację aktualizacji systemu Windows automatyzuje i przyspiesza instalację nowych aktualizacji systemu Windows
- Pokazuj ostrzeżenia o problemach z dyskami fizycznymi włącza powiadomienia informujące o problemach w działaniu dysków fizycznych w przypadku, gdy takie problemy są raportowane w systemie
- Pokazuj ostrzeżenia o kończących się zasobach włącza powiadomienia informujące o zbyt małych zasobach dostępnych dla systemu, np. w przypadku kończącego się miejsca na dysku
- 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" 2, 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

m	mks_vir a	administrator		-		×
	**	Zarządzane s	admine 127.0.0.1	Ustav	vienia	1
	U		Szybka konfiguracja			
	Q		✤ Tryb wydajny			
	Ť		Tryb optymalny			
		aktualizacja	Tryb paranoiczny			
		android	Ustawienia użytkownika			
			Za	mknij		l
			■ ×			

D – 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:

m	mks_vir	administrator		-		х
	-		admin@127.0.0.1			
1	<b>2</b> 2	Zarządzane s <sup>(grupa)</sup>	stacje	Ustaw	ienia	
4	U	ochrona	Zmiana serwera zarządzającego			
1	Q	skanowanie	Stacja/stacje zostaną przeniesione do wskazanego poniżej serwera zarządzającego.			I
1	•	kontrola	Nowy serwer zarządzający (serwer:port):			^
		rodzicielska	Numer licencji			J.
1	*	aktualizacja	Jeśli pole numeru licencji będzie puste stacja/stacje będą korzystały z dotychczasowego klucza.			l
l	*	ogólne	Numer licencji: Podgląd pulpitu			l
l	÷	android	□ Pytaj o zezwolenie na podgląd pulpitu □ Blokuj podgląd miniatury pulpitu			l
1	8	zarządzanie	Dowiedz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitow			I
1						I
1						I
l						
1	_		🖅 Grupa nie ma zdefiniowanego własnego numeru licencji Zmień numer li	cencii		

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

Numer licencji – umożliwia szybką aktualizację/zmianę licencji na stacjach

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

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

## 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  $\rightarrow$  Urządzenia  $\rightarrow$  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):

m	mks_vir administrator		-		Х
	Szczegóły urządze	nia USB			
	Etykieta urządzenia:	Urządzenie USB			
	Producent:				
	Produkt:				
	Klasa:				
	Opis:				
	Numer seryjny:				
		Dodaj urządzenie z listy			
	ОК	Δ	nuluj		
			_	-	

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

						ministrator	miks_vir au
$\mathbf{\Theta}$			h w sieci	atnio aktywnyd	zeń USB ost	Lista urządz	●┤╸
	Czas	Opis	Klasa	Produkt	Producent	Użytkownik	Maszyna
۹	2023.07.04 08:44:15	USB Mass Storage Device	USB	SanDisk 3.2Gen1	USB	tester	TEST01
۹	2023.07.04 08:44:23	USB Attached SCSI (UAS) Mass Storage Device	SCSIAdapter	Portable SSD	Intenso	tester	TEST01
	2023.07.04 08:44:15 2023.07.04 08:44:23	USB Mass Storage Device USB Attached SCSI (UAS) Mass Storage Device	USB SCSIAdapter	SalTUSK 3.2Gen1 Portable SSD	USB	tester tester	TESTOI

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):

m	mks_vir administrator		-		×
	-		_	_	
	Szczegóły urządze	nia USB			
	Etykieta urządzenia:	Intenso/Portable SSD/SCSIAdapter/2023.07.04 08:56:14			
	Producent:	=Intenso			
	Produkt:	=Portable SSD			
	Klasa:	=SCSIAdapter			
	Opis:	=USB Attached SCSI (UAS) Mass Storage Device			
	Numer seryjny:	=2017082715094			
		Dodaj urządzenie z listy			
	ОК	Α	nuluj		
	_		_		

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  $\rightarrow$  Pokaż listę reguł użytkownika":

m	mks_vir a	dministrator										-		х
		Zarządzane s <sup>(grupa)</sup>	tacje									Ustav	vienia	
	U		✓ A Tr	ktywuj konti Lista regu	rolę rodzi ł użytko	icielską wnika	-	-	-					
	Q		0			Reguła		Za	kres	A	kcja		١Į	
	Ť	kontrola rodzicielska	0										1	
	*		N N N										1	
	*		Ha										ł	-
													1	
													1	
						_							. I	
			I.	Dodaj	regułę	_	 			_	Zar	nknij	Ц	
							×							
1														

Aby utworzyć własną regułe 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:

m	mks_vir a	dministrator										-		×
1	**	Zarządzane s <sup>(grupa)</sup>												1
	U		✓ A Tr	ktywuj kontro Lista reguł	lę rodzici Jżytkow	elską nika	-	-			-			
	Q		0			Reguła			Zakres	Akcja			U.	
	Ť	kontrola rodzicielska	0						Adres	Blokuj	•	)		
	Ł													
	*		Ha										ł	-
			I.	Dodaj re	gułę		_			_	Zamkni	J	Ц	
						[	B	×					ĺ	l
	_													

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. Kolejość zdefiniowanych reguł można zmieniać za pomocą strzałek  $\uparrow i \downarrow$  (po prawej stronie), w przypadku konieczności usunięcia reguły wystarczy wybrać znak  $\otimes$  (również po prawej stronie).

Przykładowa lista zdefiniowanych własnych reguł może wyglądać nastepująco:

m mks_vir	administrator							-		×
*	Zarządzane s <sup>(grupa)</sup>									1
		⊡ AI Tr	ktywuj kontrolę rodzicielską Lista reguł użytkownika	-	-			-		
Q		0	Reguła			Zakres	Akcja		• I	
•	kontrola	0	google.pl			Adres	Pozwól	€ ⊕ (	9	
		0	google.com			Adres	Pozwól	€ ⊕ (	9	
÷			amazon-adsystem.com			Adres	Blokuj	€ € (	Ð	
		<b>V</b>	doubleclick.net			Adres	Blokuj	¢ ک 🐑	)	
		Hē	creative-serving.com			Adres	Blokuj	(*)	)	
*		0	Dodaj regułę		_		Z	amknij		
				B	×					

# 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:

mks_vir administrator	- D X
mks_Vır	admin@127.0.0.1 25/0/4000 Repozytorium: 2024.05.29 10:09:33
Zarządzane stacje     STACJE     STACJA1     STACJA2     STACJA2     STACJA3     STACJA4     SERWER ★	STACJA4       Itester       Windows 11 Pro         stacja       ustawienia       raporty       oprogramowanie         Image: Stacja jest bezpieczna       Podstawowe informacje o stacji       Image: Stacja jest bezpieczna
	Nazwa stacji:         TEST04 [10623119-0edf-b338-27b257644be0]           Adres:         10.0.0.104 [2c105d7c79a7]           Procesor:         05%         11nte(IP) Core(TM) I3-9100 CPU @ 3.60GHz           Pamięć:         16%         16246MB           Dyski:         C         118 G9 85 GB         2 931 G9 874 GB           Miejsce do odzyskania         653.51 MB         C         2 931 G9 874 GB           Oczekujące aktualizacje:         2         2         2
	Numer licencji:         TESTY-789B-BA94-A202-2011-0B0C-1087-D108-7F1E-10K1-G1H1-Z5           Licencja:         217           Wersja bazy:         2024-05-29 09:03:21           Dodatkowe informacje:         Akcje
	Aktualizacja     Wyłącz stację     Menadżer procesów       Skanowanie szybkie     Włacz stacje     Zdalny pulpit (RDP)
	Q Skanowanie pełne 🖸 Restartuj stację 💿 Podgląd pulpitu (*)
	Wyczyść SafeStorage     A Zablokuj stację     Wyślij wiadomość
	The second secon
	Wydajność systemu
	(*) Dowledz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitów

2. wybieramy "Audyt systemu":

stacja stacja Podst mks_vir przesyja przesyja audytu a Proces g kontynuc	Repozyto STACJA4 ustawienia rapo Stacja jest bezpieczna tawowe informacje o sta administrator - pytanie vstemu jest szczegółowy ny bezpośrednio do Dził ecjalistów od bezpieczeń dres e-mail pozwala na u enerowania audytu syst wać?	admin@1 23/0/- rium: 20: tes rty c acji mr raport stwa ko istwa ko istwa ko izyskanie emu mo.	127.0.0.1 4000 24.05.29 10:09:33 ster • • • • • • • • • • • • • • • • • • •	Vindows 1 S_Vir I ana ny przy w nalizie). Czy chces	taport ten jest ližovany vsykaniu z	. *	•	0
stacja stacja Podst mks_vir Audyt sy przesyła przez Sp audytu a Proces 9 kontynuc	STACJA4 (tacp) ustawlenia rapo Stacja jest bezpieczna tawowe informacje o sta administrator - pytanie (stemu jest szczegółowy ny bezpośrednio do Dzie ecjalistów od bezpieczeń dreś se -mal pozwala na u enerowania audytu syst	rty o acji wm raport łu Wspa istwa koi sistwa koi sistwa koi sistwa koi sistwa koi sistwa koi sistwa koi	ster • <b>W</b> v oprogramowanie tem o stanie systemu W arcia Technicznego Ma mputerowego (podawa e odpowiedzi po jego ar że potrwać kilka minut.	Vindows 1 Vindows, F s_vir i ana ny przy w alizie), zzy chces	taport ten jest liizowany ysylaniu z	]		
stacja Podst mks_vir Audyt sy przesyła przez sy audytu a Proces g kontynuc	ustawienia rapo Stacja jest bezpieczna tawowe informacje o sta administrator - pytanie stemu jest szczegółowy ny bezpośrednio do bezpieczeń dreś se-mal pozwala na u enerowania audytu syst wac?	rty o acji fm rapori stwa kol istwa kol zyskanie emu mo:	tem o stanie systemu V arcia Technicznego mk mputerowego (podawa e odpowiedzi po jego ar że potrwać kilka minut.	vindows. F s_vir i ana ny przy w alizie). Czy chces	laport ten jest liizowany systaniu z			
Podst mks_vir Audyt sy przesyła przez Sp audytu a Proces g kontynuc	administrator - pytanie administrator - pytanie ystemu jest szczegółowy ny bezpośrednio do Dzie ecjalistów od bezpieczeł dreś se -mai pozwala na u enerowania audytu syst ować?	m rapori istwa ko izyskanie emu moż	tem o stanie systemu W arcia Technicznego mk mputerowego (podawa e odpowiedzi po jego ar że potrwać kilka minut.	Vindows. F s_vir i ana ny przy w nalizie). Czy chces	Paport ten jest lilzowany ysyłaniu z			
mks_vir Audyt sy przesyła przez Sp audytu a Proces g kontynuc	administrator - pytanie ystemu jest szczegółowy ny bezpośrednio do Dzie cejalistów od bezpieczeń dres e-mail pozwala na u enerowania audytu syst wać?	rm rapori a <b>łu Wspa</b> istwa ko izyskanie <b>emu</b> moż	tem o stanie systemu W arcla Technicznego mk mputerowego (podawa e odpowiedzi po jego ar że potrwać klika minut.	vindows. F s_vir i ana ny przy w nalizie). Czy chces	Paport ten jest Ilizowany ysyłaniu z			
Audyt sy przesyła przez Sp audytu a Proces g kontynuc	ystemu jest szczegółowy ny bezpośrednio do Dzia ecjalistów od bezpieczer dres e-mail pozwala na u enerowania audytu syst ować?	rm rapor a <b>łu Wspa</b> istwa ko izyskanie emu moż	tem o stanie systemu W arcia Technicznego mk mputerowego (podawa e odpowiedzi po jego ar że potrwać kilka minut.	Vindows. F s_vir i ana ny przy w nalizie). Czy chces	aport ten jest Ilizowany ysyłaniu z			
	Nie			Ta	k	-Z5		
k	Skanowanie szybkie		Włacz stacio		Zdalny pulpit (	sów		
0	Skanowanie pełne	2	Restartui stacie	ų O	Podglad pulpit	tu (*)		
∼ m	Wyczyść <i>SafeStorage</i>	Ĩ	Zablokuj stację		Wyślij wiadom	ność		
5	Kwarantanna	<u>lıl</u>	Audyt systemu Wydajność systemu	Ŷ	Uruchom proc	ces		
	- <b>*</b> Q 🗇 🛧	Nie       %     Skanowanie szybkie       Q     Skanowanie pełne       Image: Wyczyść SafeStorage       %     Kwarantanna	Nie Skanowanie szybkie Skanowanie pełne Wyczyść <i>SafeStorage</i> Kwarantanna Mu	Nie     Viącz stację       Skanowanie szybkie     O Wiącz stację       Skanowanie pełne     Z Restartuj stację       Wyczyść SafeStorage     Zablokuj stację       Kwarantanna     Jul Audyt systemu       Wydajność systemu     Wydajność systemu	Nie     Transmitter       Ý     Skanowanie szybkie     O     Wiącz stację       Q     Skanowanie pełne     Z     Restartuj stację       Image: Wyczyść SafeStorage     Image: Audyt systemu     Image: Audyt systemu       Image: Wycdylowie wydajność systemu     Image: Audyt systemu	Nie     Tak <sup>4</sup> Skanowanie szybkie Q. Skanowanie pełne <sup>10</sup> Wyczyść <i>SafeStorage</i> <sup>10</sup> Kwarantanna <sup>10</sup> Włącz stację <sup>10</sup> Restartuj stację <sup>10</sup> Zablokuj stację <sup>10</sup> Xudyt systemu <sup>11</sup> Audyt systemu <sup>11</sup> Wydajność systemu <sup>11</sup> Uruchom processor <sup>11</sup> Wydajność systemu	Nie     Tak       Ý     Skanowanie szybkie          〇     Włącz stację           Zdalny pulpit (RDP)        Q     Skanowanie pełne          ②     Restartuj stację           Podgląd pulpitu (*)        Im     Wyczyść SafeStorage          Q     Zablokuj stację           Wyślij władomość        Im     Audyt systemu          Q     Uruchom proces        Im     Wydajność systemu          Wydajność systemu	Nie     Tak       %     Skanowanie szybkie <ul> <li>Wiącz stację</li> <li>Zdalny pulpit (RDP)</li> <li>Skanowanie pełne</li> <li>Restartuj stację</li> <li>Podgląd pulpitu (*)</li> <li>Wyczyść <i>Safestorage</i></li> <li>Zablokuj stację</li> <li>Wyśli władomość</li> <li>Kwarantanna</li> <li>Audyt systemu</li> <li>Vurdamość systemu</li> </ul>

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

e-mail kontaktowy:	moj_email@moja.domena		_
temat wiadomości:	System audit		
wiadomość / opis problemu:	Opis problemu	 	
pliki do wysłania / załączniki:	Dodaj plik		
[] C:\ProgramData\mks_vir\tmp\auc	lit_106231f9-0edf-b338-27b257644be0_20240529111731.zip		

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):

mks_vir administrator	- 🗆 X
admin@12 Ustawienia konsoli i serwera zarządzającego	7.0.0.1
Żródło aktualizacji repozytorium dla stacji Stacje zarządzane z poziomu konsoli administracyjnej mks_vir domyśnie aktualizują się z repozytorium udostępnianego przez serwer zarządzający mks_vir. Poniżej możesz podać adres zasobu (http albo lokalnego), na podstawie którego serwer zarządzający mks_vir tworzy repozytorium aktualizacyjne dla stacji. Puste pole oznacza serwer aktualizacji mks_vir. Adres serwera źródłowego:	Żródło aktualizacji serwera zarządzającego Adres, z którego ma być aktualizowany serwer mks_vir. Puste pole oznacza serwer aktualizacji mks_vir. Adres serwera źródłowego:
Konta	Ustawienia powiadomień Pokaż ustawienia powiadomień email Pokaż ustawienia powiadomień Syslog Ustawienia dodatkowe Zamykaj konsolę po 5 minutach nieaktywności
	×

po czym kliknąć w "Dodaj użytkownika":

mks_vir administrator	- 🗆 X
admin@127.	0.0.1
Źródło aktualizacji repozytorium dla stacji	Źródło aktualizacji serwera zarządzającego
Stacje zarządzane z poziomu konsoli administracyjnej mks_vir domyślnie aktualizują się z repozytorium udostępnianego przez	Adres, z którego ma być aktualizowany serwer mks_vir. Puste pole oznacza serwer aktualizacji mks_vir.
(http://dxalacajdczijdcy/mks_vir. Ponizej mozesz podac adres zasobu (http://dxalanego), na podstawie którego serwer zarządzający mks_vir tworzy repozytorium aktualizacyjne dla stacji.	Adres serwera źródłowego:
Puste pole oznacza se Nowy użytkownik	
Adres serwera źródłow Nazwa użytkownika :	
Konta Hasło :	
Dodaj użytke     Powtórz hasło :	nail 🛈 🔤 🔤
admin	slog 🔿
Δημμί	
	<u> </u>
	<b>^</b>

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

mks_vir administrator	- 🗆 X
admine 12 Ustawienia konsoli i serwera zarządzającego	7.0.0.1
Źródło aktualizacji repozytorium dla stacji Stacje zarządzane z poziomu konsoli administracyjnej mks_vir domyślnie aktualizują się z repozytorium udostępnianego przez serwer zarządzający mks_vir. Poniżej możesz podać adres zasobu (http abo lokalnego), na podstawie którego serwer zarządzający mks_vir tworzy repozytorium aktualizacyjne dla stacji. Puste pole oznacza serwer aktualizacji mks_vir. Adres serwera źródłowego:	Żródło aktualizacji serwera zarządzającego ✓ Adres, z którego ma być aktualizowany serwer mks_vir. Pustę pole oznacza serwer aktualizacji mks_vir. Adres serwera źródłowego:
Konta       Line     Zmlana hasta     Usuń       admin     C     Image: Constraint of the second seco	Ustawienia powiadomień  Pokaż ustawienia powiadomień email  Fier Pokaż ustawienia powiadomień Syslog  Ustawienia dodatkowe  Zamykaj konsolę po 5 minutach nieaktywności
B	×

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

m mks_vir administrator	Repozyto	admin@127.0.0.1 20/0/4000 rium: 2024.05.29 10:09:33	Q 🕹 🕯	□ × ₽ ₽
Arządzane stacje     GRUPA1     GRUPA2     GRUPA2	GRUPA1 (grupa)         grupa       ustawienia         rapo         Stacje w grupie są bezpi         W grupie są stacje z ocz         Podstawowe informacje o gr	rty oprogramowanie eczne ekującymi aktualizacjami W upie	podsumowanie Indows	
	Liczba stacji w grupie: 2 Zakres wersji baz: 2024 Zakres abonamentów: 217 Uprawnienia: admi Akcje	-05-29 09:03:21 n ☑		
	🛃 Aktualizacja	Wyłącz stacje	Menadżer procesów	
	Skanowanie szybkie	Włącz stacje	Czyszczenie systemów	
	Q Skanowanie pełne	🕻 Restartuj stacje	Wyślij wiadomość	
	Wyczyść SafeStorage	Zablokuj stacje	Uruchom proces	
	🛧 Wyczyść kwarantannę		Podgląd pulpitów (*)	
	(*) Dowledz się więcej o możliwości	dodatkowej konfiguracji podgląc	tu pulpitów	

po czym kliknąć ikonę 🗹 w linii "Uprawnienia":

m mks_vir administrator		– 🗆 X
mks_Vır	admin@127.0.0.1 23/0/4000 Repozytorium: 2024.05.29 10:09:33	Q 🕇 🌣 🖯
Zarządzane stacje     GRUPA1     GRUPA1     GRUPA1	GRUPA1 (grupa)	
GRUPA2	grupa ustawienia raporty oprogramowanie podsumowanie Uprawnienia dla grupy: GRUPA1	
STACJA3	Użytkownik Dostęp user1 v user2 x	
		sów
		temów
		ŝĈ
		v (*)
	Anuluj Zapisz 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:

	Repozvic	user1@127.0.0.1 30/2/4000 ritum: 2024 05 29 10:09:33	⊂ - □	× 8
Zarządzane stacje	GRUPA1 (grups)         grupa       ustawlenia       rapo         Stacje w grupie są bezp         W grupie są stacje z ocz         Podstawowe informacje o gr         Liczba stacji w grupie:       2         Zakres wersji baz:       2024         Zakres wersji baz:       2024         Zakres abonamentów:       217	oprogramowanie ieczne ekującymi aktualizacjami Wi upie -05-29 09:03:21	podsumowanie ndows	
	Aktualizacja         Skanowanie szybkle         Skanowanie pełne         Wyczyść SafeStorage         Wyczyść kwarantannę         Wyczyść kwarantannę         (*) Dowiedz się więcej o możliwości	<ul> <li>Wyłącz stacje</li> <li>Wiącz stacje</li> <li>Restartuj stacje</li> <li>Zablokuj stacje</li> </ul>	<ul> <li>Menadžer procesów</li> <li>Czyszczenie systemów</li> <li>Wyślij Wiadomość</li> <li>Uruchom proces</li> <li>Podgląd pulpitów (*)</li> </ul>	

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  $\Theta$  programu **mks\_vir administrator** i wybrać *"Zarządzanie bazą"*.

m mks_vir administrator - zarządzanie bazą			_		×
Baza danych					
Rozmiar bazy: 757 KB	Wyczyść bazę	Usuń nieaktywne s	tacje		
Kopie zapasowe					
€ 2022.11.25 09:19:39	37.8 KB	<b>C</b> 🖹 🛍			
2022.11.25 09:10:33	6.5 KB	<b>2</b> 🖪 🖻			
2022.11.25 09:09:23	6.5 KB	<b>2</b> 🖹 🛍			
2022.11.25 09:07:09	6.1 KB	<b>2</b> 🖪 🛍			
2022.11.22 12:02:37	1.8 KB	<b>2</b> 🗈 🖻			
2022.11.22 11:57:02	1.8 KB	<b>2</b> 🗈 🖻			
2022.11.22 11:33:53	2.6 KB	<b>2</b> 🖪 🖻			
2022.11.22 11:25:59	787 B	<b>2</b> 🖪 🖻			
🗆 Pełna kopia bazy					
Twórz kopię zapasową	Odtwórz kopię za	apasową	Zai	mknij	

#### 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)

m mks_vir administrator -	zarządzanie bazą	_		×
Baza danych				
Rozmiar bazy:	757 KB Wyczyść bazę Usuń nieaktywne stacje			
Kopie zapasowe				
2022.11.25 09:				
2022.11.25 09:	Usuwanie nieaktywnych stacji			
2022.11.25 09:				
2022.11.25 09:	Z bazy zostaną usunięte stacje, które nie zgłosiły się do serwera przez wskazaną poniżej liczbę dni:			
2022.11.22 12:0				
2022.11.22 11:5	30			
2022.11.22 11:3				
2022.11.22 11:2				
	Anuluj Usuń nieaktywne stacje			
🗌 Pełna kopia bazy				
Twórz kopię za	pasową Odtwórz kopię zapasową	Zai	mknij	

### 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":

mks_vir administrator	- 0
admin@12	7.0.0.1
Ustawienia konsoli i serwera zarządzającego	
Źródło aktualizacji repozytorium dla stacji	Źródło aktualizacji serwera zarządzającego
Stacje zarządzane z poziomu konsoli administracyjnej mks_vir domyślnie aktualizują się z repozytorium udostępnianego przez serwer zarządzający mks_vir. Poniżej możesz podać adres zasobu	Adres, z którego ma być aktualizowany serwer mks_vir. Puste pole oznacza serwer aktualizacji mks_vir.
(http albo lokalnego), na podstawie którego serwer zarządzający mks_vir tworzy repozytorium aktualizacyjne dla stacji.	Adres serwera źródłowego:
Puste pole oznacza serwer aktualizacji mks_vir.	
Adres serwera źródłowego:	
Konta	Ustawienia powiadomień
🚑 Dodaj użytkownika	🖸 Pokaż ustawienia powiadomień email 👁
Użytkownik Zmlana hasła Usuń admin 🕹	🗮 Pokaż ustawienia powiadomień Syslog 🕥
	Ustawienia dodatkowe
	🗹 Zamykaj konsolę po 5 minutach nieaktywności
	×
Comma nie ma gdofiniowanogo v	Zmioń pupor liconcii

Uruchomi się okno konfiguracji powiadomień:

Źródło aktualizacji rep	ozytorium dia sta	acji		Źródło aktualizacji se	erwera zarządzająco	ego	
Stacle zarządzane comyśnie aktualizują r ichty alto aktualizują r ichty alto kalniego, mks_vir tworzy repoz Puste pole oznacza se Adres serwera źródłow Konta Lytkownik Zmłan admin z	Ustawienia Powiadamia Serwer : Port : Szyfrowanie : Użytkownik : Hasło : Nadawca : Adresaci : Temat : Filtry :	a powładom anie aktywne 587 STARTTLS	wiadomienie	0		nail () slog () ości	

gdzie należy zaznaczyć opcję "Powiadamianie 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":

:
7.0.0.1
Żródło aktualizacji serwera zarządzającego Adres, z którego ma być aktualizowany serwer mks_vir. Puste pole oznacza serwer aktualizacji mks_vir. Adres serwera źródłowego:
Ustawienia powiadomień
<ul> <li>Pokaż ustawienia powiadomień email </li> <li>Pokaż ustawienia powiadomień Syslog </li> <li>Ustawienia dodatkowe</li> </ul>
Zamykaj konsolę po 5 minutach nieaktywności
*

Uruchomi się okno konfiguracji powiadomień:

m	mks_vir administrator		-		×
	Ústawienia konsoli         Źródło aktualizacji repr         Ś Stacje zarządzane domyślnie aktualizują serwer zarządzający mks_vir tworzy repoz         Puste pole oznacza se Adres serwera źródłow         Konta         Lodaj użytko         Użytkownik       Zmłan admin	serwera zarządzającego   zzytorium dla stacji   Źródło aktualizacji serwera zarządzającego   Ustawienia powiadomień Syslog   Powładamianie aktywne   Serwer :   Port :   514   Protokół :   TCP 🔍   Format logu :   RFC 5424 (IETF) 🔍   Filtry :	nail () slog () pści	_vir.	
		Anuluj OK	er licencii		

gdzie należy zaznaczyć opcję "Powiadamianie 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)

<b>RFC 5424 (IETF)</b>	
RFC 3164 (BSD)	

• 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"

# 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":

mks_vir administrator - zarządzanie bazą		-		Х
Baza danych				
Rozmiar bazy: 8 MB	Wyczyść bazę			
Kopie zapasowe				
2022.01.26 14:53:42	26.4 КВ 🛛 🔁 🖻			
🗌 Pełna kopia bazy				
Twórz kopię zapasową	Odtwórz kopię zapasową	Za	mknij	

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 **II**:

Baza danych → Rozmiar bazy: 8 MB Wyczyść bazę Kopie zapasowe 2012 0127 11:50:42 • 221 KB 7 €		
Rozmiar bazy: 8 MB Wyczyść bazę Kopie zapasowe		
Kopie zapasowe         2012 01 27 11:50:42         201 KB         2 ID         ⊕		
🛢 2022.01.27.11·50·42 🍙 291.KB 🗖 🖪 🎰		
STATE STATE STATE STATE		
🛢 2022.01.26 14:53:42 26.4 KB 🔀 🖺 🗎		
🗆 Pełna kopia bazy		

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":

mks_vir administrator - zarządzanie baz	ą		_	>
Rozmiar bazy: 90 KB	Wyczyść bazę			 
Kopie zapasowe				
2022.01.27 12:46:01	23.4 KB	<b>2</b> 🖪		
Pełna kopia bazy				

 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:

<b>—</b> • • • • • • • • • • • • • • • • • • •		_	~
III mks_vir administrator - zarządzanie bazą	-	U	~
Baza danych			
Rozmiar bazy: 90 KB Wyczyść bazę			
Kopie zapasowe			
2022.0 Zarządzanie bazą - pytanie			
Czy chcesz odtworzyć tę kopię zapasową i nadpisać aktualną wersję bazy?			
Nie Tak			
Peina kopia bazy			
Twórz kopię zapasową         Odtwórz kopię zapasową	Zai	mknij	

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":

m mks_vir administrator - zarządzanie bazą				-		×
Baza danych						
Rozmiar bazy: 8 MB	Wyczyść bazę	]				
Kopie zapasowe						
2022.01.26 14:53:42	26.4 KB	<b>2</b> 🖻 🖻				
<b>—</b>						
🗆 Pełna kopia bazy						
Twórz kopię zapasową	Odtwórz kopię	zapasową	[	Zai	mknij	

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 **II**:

m mks_vir administrator - zarządzanie bazą			- 🗆 X
Baza danych			
Rozmiar bazy: 8 MB	Wyczyść bazę	]	
Kopie zapasowe			
2022.01.27 11:50:42	381 KB	<b>2</b> 🗈 🖮	
2022.01.26 14:53:42	26.4 KB	<b>2</b> 🖹 🛍	
🗌 Pełna kopia bazy			
Twórz kopię zapasową	Odtwórz kopię	zapasową	Zamknij

 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":

 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:

mks_vir adn	iinistrator - zarządzanie bazą	-		×
Baza danyc	'n			
Rozm	lar bazy: 90 KB Wyczyść bazę			
(opie zapa:	owe			
2022.0	Zarządzanie bazą - pytanie			
	Czy chcesz odtworzyć tę kopię zapasową i nadpisać aktualną wersję bazy?			
			_	

- 3. po zakończeniu odtwarzania bazy zamykamy program zarządzający bazą
- 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":
| m | mks_vir a | administrator                      |  | -      |        | × |
|---|-----------|------------------------------------|--|--------|--------|---|
|   | _         |                                    | admin@127.0.0.1  |        |        |   |
|   | 202       | Zarządzane :<br><sup>(grupa)</sup> | stacje   | Ustav  | vienia |   |
| 4 | U         | ochrona                            | Zmiana serwera zarządzającego  |        |        |   |
|   | Q         | skanowanie                         | Stacja/stacje zostaną przeniesione do wskazanego poniżej serwera zarządzającego.               |        |        | ] |
|   | •         | kontrola                           | Nowy serwer zarządzający (serwer:port):  |        |        |   |
|   |           | rodzicielska                       | Numer licencji   |        |        | : |
|   | *         | aktualizacja                       | Jeśli pole numeru licencji będzie puste stacja/stacje będą korzystały z dotychczasowego klucza |        |        |   |
|   |           |                                    | Numer licencji:  |        |        | I |
|   |           | ogóine                             | Podgląd pulpitu  |        |        | J |
|   | ŵ         | androld                            | □ Pytaj o zezwolenie na podgiąd pulpitu<br>□ Blokuj podgląd miniatury pulpitu                  |        |        | I |
|   |           |                                    | Dowledz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitów                      |        |        | I |
|   |           | zarządzanie                        |  |        |        | I |
|   |           |                                    |  |        |        | I |
|   |           |                                    |  |        |        | I |
|   |           |                                    |  |        |        | L |
|   |           |                                    |  |        |        | L |
|   |           |                                    |  |        |        |   |
|   | _         |                                    | 🖅 Grupa nie ma zdefiniowanego własnego numeru licencji Zmień nymerki                           | cencii |        |   |

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:

 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* 

 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

 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 spowodwać 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 umożliwające rozpoczęcie instalacji programu:



Po wybraniu "Kontynuuj", zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku "Kontynuuj":



pojawi się okno do wpisania numeru licencji:

mks_Vır	
NUMER LICENCJI	
Podaj numer licencji pakietu mks_vir:	
1	

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:

ARZĄDZANIE PAKIE	ΓEM	
eśli chcesz, żeby stacja b dres serwera i numer po	yła zarządzana z poziomu serw rtu komunikacyjnego	era mks_vir administrator, wpisz poniże
śli stacja ma nie być za	ządzana, pozostaw pole <b>Adres</b>	<b>serwera</b> puste.
Adres serwera:		
Port komunikacyjny:	4000	
☑ Sprawdź połączen	ie z serwerem przed kontynu	acją instalacji

Rozpocznie się właściwa instalacja pakietu:



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

mks_Vr	_×
INSTALACJA ZAKOŃCZONA	
Instalacja została zakończona. Program jest gotowy do pracy.	
Wersja programu instalacyjnego: 2018.01.09 12:54:01	
	Zakończ

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 najwięk-szą ilością wolnego miejsca):

_	mks	vir			
	TIKS_	VII			_
	m	ks_		Nersja bazy wirusów: 2018.01.09 12:4	11:36 💵 Licencja: 353 dni
	Dys	k dla d	anych programu	ı mks_vir	
	W sy poter	stemie je: ncjalnie di	st dostęnych kilka dys uże ilości danych (Saf	sków. Wskaż, na którym dysku prog eStorage, kwarantanna itp.):	ram mks_vir ma przechowywać
		C:\	Pojemność dysku: Wolne miejsce:	111 GB 97 GB	DYSK SYSTEMOWY
		D:\	Pojemność dysku: Wolne miejsce:	465 GB 327 GB	
					Kontynuuj

# 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 umożliwające rozpoczęcie instalacji programu:

Zamknij Kontynu	uj
Wersja programu instalacyjnego: 2018.01.02 13:21:41	
w trakcie instalacji w systemie zostaną zainstalowane wszystkie komponenty niezdędne do pracy serwera zarządzającego mks_vir.	
Witamy w programie instalacyjnym pakietu mks_vir administrator.	
WITAMY	
	_X

Po wybraniu "Kontynuuj", zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku "Kontynuuj":

	CENCIJINA	
Poniższa umow Producentem, i programu anty (Ustawa o Praw postanowienia postanowienia Umowie. Przyjr nie akceptuje v ono nabyte w z Nabywca ma p Producent zast reklamowych o promocjach pro	a przedstawia postanowienia prawne zawarte pomiędzy firmą Arcabit Sp. z o.o. zwaną dalej a Nabywcą jako końcowym użytkownikiem. Firma Arcabit Sp. z o.o. jest producentem wirusowego mks_vir, zwanego dalej Programem. Jest on chroniony przez prawo polskie ie Autorskim i Prawach Pokrewnych Dz. U. Nr 24, poz. 83) oraz międzynarodowe o ochronie własności intelektualnych i prawnych. sprzedaje Nabywcy Programu, a jedynie udziela mu prawa jego użytkowania zgodnie z mi niniejszej Umowy. Producent zastrzega sobie wszelkie prawa nie wyrażone bezpośrednio w nuje się, że Nabywca instalując program, akceptuje postanowienia tej umowy. Jeśli Nabywca rarunków umowy w ciągu 30 dni może zwrócić oprogramowanie w miejscu, gdzie zostało ramian za zwrot zapłaconej kwoty w pełnej wysokości. Po upływie okresu aktualizacji rawo do wykorzystywania Programu bez prawa do aktualizacji. rzega sobie prawo dołączenia do aktualizacji Programu materiałów informacyjno współpracujących z nim podmiotach trzecich oraz przesyłania informacji o produktach i poducenta.	
Nabywca ma j	Jrawo:	,

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:

USTAWIENIA	SERWERA	
• Numer portu,	, który będzie wykorzystywany do komunikacji stacji z serwerem.	
Uwaga: Do kom podanego.	unikacji będą wykorzystywane w sumie 4 kolejne porty począwszy od portu	
Numer portu:	4000	
• Hasło użytko Hasło:	wnika administracyjnego (admin) pakietu mks_vir administrator	
• Hasło użytko Hasło: Powtórz hasło:	wnika administracyjnego (admin) pakietu mks_vir administrator	
• Hasło użytko Hasło: Powtórz hasło:	wnika administracyjnego (admin) pakietu mks_vir administrator	

Po wybraniu przycisku "Kontynuuj" rozpocznie się właściwa instalacja pakietu:

<b>mks_VIF</b> 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 umożliwające rozpoczęcie instalacji programu:

mks_Vır	_×
WITAMY	
Witamy w programie instalacyjnym pakietu mks_vir. W trakcie instalacji w systemie zostaną zainstalowane wszystkie komponenty niezbędne do pracy programu i ochrony systemu.	
Wersja programu instalacyjnego: 2018.01.02 13:22:27	
Zamknij Kontynuuj	

Po wybraniu "Kontynuuj", zatwierdzeniu umowy licencyjnej i ponownym wybraniu przycisku "Kontynuuj":



pojawi się okno do wpisania numeru licencji:

mks_Vır		_×
NUMER LICENCJI Podaj numer licencji pakietu mks_vir:		
Wersja programu instalacyjnego: 2018.01.02 13:22:27		
Zamknij	Wstecz	Kontynuuj

Po wpisaniu numeru licencji i zatwierdzeniu przyciskiem "Kontynuuj" wybieramy folder instalacyjny **mks\_vir** (sugerujemy pozostawienie domyślnego), po czym ponownie wciskamy przycisk "Kontynuuj":

mks_Vr			_>
ŚCIEŻKA INSTALACYJNA			
Folder instalacyjny pakietu mks_vir			
		Zimentolder	
Versja programu instalacyjnego: 2018.01.02 13:22:27			
Zamknij	Wstecz	Kontynu	uj

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**):

ARZADZANIE PAKIE	TFM	
śli chcesz, żeby stacja b łres serwera i numer po	była zarządzana z poziomu ortu komunikacyjnego.	serwera mks_vir administrator, wpisz poniże
śli stacja ma nie być za	rządzana, pozostaw pole <b>A</b>	<b>dres serwera</b> puste.
Adres serwera:	server	
Port komunikacyjny:	4000	
☑ Sprawdź połączen	ie z serwerem przed kont	ynuacją instalacji

**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:

mks_Vır	_×
INSTALACJA	
bases\pc\cat05.bin	
Wersja programu instalacyjnego: 2018.01.02 13:22:27	

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 przejrzenie raportów z działania programu mks\_vir

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

Orange uttali 🕹 🕅 Plus 👘 all 🔒 🕅	\$64% 💷 12:22		
mks_Vır	Skanowanie		
(app)com.huawei.browser			
Przeskanowane obiek	ty: 20		
	ZAKOŃCZ		

Po wybraniu Aktualizacji pojawia się okno wyświetlające status aktualizacji programu mks\_vir:



		WRÓĆ
$\triangleleft$	0	

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 zarzadzającego mks\_vir administrator (domyślnie 4000)

Po wybraniu **Raportów** pojawia się okno umożliwiające przejrzenie 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;
- 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:

- 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 jakiejkolwiek 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 przesyłać 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 jakiekolwiek 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 uiścił za licencję na korzystanie z programu.