# 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			-	×
	mks_VII	<u></u>		
	Logowanie do	serwera		
	Adres serwera:	127.0.0.1		
	Port:	4000		
	Użytkownik:	admin		
	Hasło:			
		Zaloguj		

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				-	×
ĺ					
	mks_VI		1500 : Błąd		
	Logowanie do	serwera 4	1502 : Błąd 1503 : Błąd		
	Adres serwera:	127.0.0.1			
	Port:	4500			
	Użytkownik:	admin			
	Hasło:				
		Zalogui			
		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

mks_vir administrator		– 🗆 X
mks_Vır	admin@127.0.0.1 12/0/4000 Repozytorium: 2024.05.29 09:03:21	Q 🕹 🌣 😡
Zarządzane stacje     STACJE     STACJE     STACJA1     STACJA2     STACJA2     STACJA3     STACJA4     SERWER *	Zarządzane stacje         grupa       ustawienia       raporty       oprogramowanie         Stacje w grupie są bezpieczne         W grupie są stacje z oczekującymi aktualizacjami W	podsumowanie Vindows
	Liczba stacji w grupie: 5 Zakres wersji baz: 2024-05-29 09:03:21 Zakres abonamentów: 217 Uprawnienia: admin ☑ Akcje	
	🛓 Aktualizacja 🕥 Wyłącz stacje	Menadżer procesów
	🕈 Skanowanie szybkie 💽 Włącz stacje	Czyszczenie systemów
	Q Skanowanie pełne 🛛 🕄 Restartuj stacje	Wyślij wiadomość
	🕅 Wyczyść SafeStorage 🔒 Zablokuj stacje	Uruchom proces
	T Wyczyść kwarantannę	Podgląd pulpitów (*)
	(*) Dowledz się więcej o możliwości dodatkowej konfiguracji podglą	du 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:

mks_vir administrator		- 🗆 X
mks_Vır	admin@127.0.0.1 23/0/4000 Repozytorium: 2024.05.29 0	Q 🕹 🏟 😧
Zarządzane stacje     STACJE     STACJA1     STACJA2     STACJA2     STACJA3     STACJA3     SSTACJA4     SERWER *	STACJE         grupa       ustawienia         color       stacje w grupie są bezpieczne         W grupie są stacje z oczekującymi aktualiza         Podstawowe informacje o grupie	wanie podsumowanie cjami Windows
	Liczba stacji w grupie: 4 Zakres wersji baz: 2024-05-29 09:03:21 Zakres abonamentów: 217 Uprawnienia: admin Z Akcje	
	🛓 Aktualizacja 🕥 Wyłącz st	acje 📑 Menadżer procesów
	🐓 Skanowanie szybkie 🛛 💽 Włącz sta	cje 🛟 Czyszczenie systemów
	Q Skanowanie pełne 🛛 🔁 Restartuj s	stacje 🗩 Wyślij wiadomość
	🗑 Wyczyść <i>SafeStorage</i> 🔒 Zablokuj s	tacje 📦 Uruchom proces
	Wyczyść kwarantannę	Podgląd pulpitów (*)
	(*) Dowledz się więcej o możliwości dodatkowej konfigurac	ji podglądu pulpitów

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

m mks_vir administrator	-		×
STACJE (grupo) Stacja Oczekujące aktualizacje STACJAL 2			8
STACJA3 1 I I STACJA4 2			
STACJA4 2 🔹			
Uruchom aktualizację s	ystemóv	N	

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

Przyciski dostępne w tej sekcji pozwalają na:

- Aktualizacja wymuszenie aktualizacji na stacjach w danej grupie
- **Skanowanie szybkie** wymuszenie wykonania skanowania szybkiego na stacjach w danej grupie
- **Skanowanie pełne** wymuszenie wykonania skanowania pełnego na stacjach w danej grupie
- Wyczyść SafeStorage usunięcie całej zawartości folderu SafeStorage na stacjach w danej grupie
- Wyczyść kwarantannę usunięcie całej zawartości kwarantanny 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):

nks_vir administrator		-
(grupa)		
Stacja Miejs	zce do odzyskania	
STACJA2	662.76 MB 👁	
STACJA3	653.44 MB 💿	
TACJA4	653.51 MB 💿	
		Uruchom czyszczenie systemó

- 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	¥	¢	8
A Zarządzane stacje	STACJE				
STACJA1 STACJA2 STACJA3 STACJA4	grupa ustawienia raporty oprogramowanie podsumowanie				
SERWER ★	Uruchomienie procesu w STACJE				
	Proces do uruchomienia:				
	Parametry:	_			
			ów mów		
	Uruchom proces z wysokimi uprawnieniami				
	Anuluj Uruchom		(*)		
	(*) Dowledz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitów		,		

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	- 🗆 X
mks_Vır	admin@127.0.0.1 21/0/4000 Q 📩 🌣 🖓 Repozytorium: 2024.05.29 09:03:21
Zarządzane stacje	STACJA1       •       •       •       •       •       •       Windows 10 Pro         stacja       ustawienia       raporty       oprogramowanie       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •       •
	Nazwa stacji:         TEST01 [09cd1307-6e1d-a880-31142113610r]           Adres:         10.0.0.101 [309c2341e24d]           Procesor:         1%           Pamięć:         556 3987MB           Dyski:         C 118 GB 95 GB 2 931GB 910 GB           Miejsce do odzyskania:         721.1 MB           Oczekujące aktualizacje:         2           Możliwy problem z dyskami:         Kilknij, żeby sprawdzlć.           Paklet mks vir         Kilknij
	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 💽 Włącz stację 📮 Zdalny pulpit (RDP)
	Q Skanowanie pełne 🔐 Restartuj stację 🕐 Podgląd pulpitu (*)
	Wyczyść <i>SafeStorage</i> Zablokuj stację <b>P</b> Wyślij wiadomość
	Trickwarantanna IIII Audyt systemu Vruchom proces
	(*) Dowledz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitów

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



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

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



Wybranie **"Uruchom 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:

			×
	2	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%			
0%			
ひ 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	ków fizycznych ADATA SU8 Parameter Raw read erro Reallocated se Power-on hou Power cycle co Power-off retr	(S.M.A.R.T.) 00 rr 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           0           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	

– Przeglądarki:

mks_vir - stan systemu			
Przeglądarki			
Strony z ustawieniami powia	adomień	(2025.06.2	4 10:36:
Wszystkie Dozwolone	Zablok	cowane Do	omyśine
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
https://www.wp.pl:443,*	Default	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

m mks_vir administrator		- 🗆 X
mks_Vır	admin@127.0.0.1 22/0/4000 Repozytorium: 2024.05.29 09:03:21	Q 🛧 🌣 🛛
Zarządzane stacje	Zarządzane stacje	
STACJE	grupa ustawienia raporty oprogramowanie podsumowanie	
STACJA3	Aktywność modułów ochronnych	
SERWER 🛨	Ochrona plików	
	Ochrona poczty	
	🗞 Ochrona przeglądarki 🌔	
	A Zapora sieciowa (firewall)	
	Y Kontrola rodzicielska	
	Kontrola urządzeń USB	
	o Kontrola urządzeń multimedialnych	
	Kontrola aplikacji	
	🗞 Ochrona rejestru	
	Ochrona w chmurze	
	Y Ochrona RoundKick EDR	
	📚 Dostęp do Internetu 💽	
	Ustawienia	
	Pokaż szczegółowe ustawienia pakietu mks_vir	
	Numer licencji	
	E Grupa nie ma zdefiniowanego własnego numeru licencji Zm	nień numer licencji

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_Vr	Repozyto	admin@ 22/0 orium: <b>2</b>	9127.0.0.1 //4000 024.05.29 10:09:33		Q	± <	* 0
Zarządzane stacje	Zarządzane stacje						
- STACJE	grupa ustawienia rapo	orty	oprogramowanie	podsumowanie			
	💡 Statystyki grupy są wylicz	zane na	podstawie raportów	o wykrytych infekcjac	h z ostatnie	ch 30 dni.	
	Eksportuj wszystkie raporty	grupy de	o pliku CSV				
	TOP 10 wykrytych infekcji w	grupie					
	Win32.Sality.OG	3					
	EICAR-Test-File (not a virus)	2			-		
	Trojan.A	1					
	Trojan.Mikey.D23070	1					
	Win32.Worm.Allaple.Gen	1					
	Win32.Virtob.Gen.12	1					
	Win32.Virtob.3.Gen	1					
	TOP 10 stacii z wykrytymi inf	lekciam	i w grupie				
	STACIA2						
	STACJAZ 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	adm 2 Repozytorium	nin@127.0.0.1 5/0/4000 h: 2024.05.29 10:09:33	Q 🛣 🌣 😡
A Zarządzane stacje     B STACJE     G STACJA1     G STACJA2	stacja ustawienia raporty	tester • Windows 10 Pro	
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	Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu Aktualizacja pakietu	
	2025-03-17 01:41:19	Aktualizacja pakietu	*
			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			– 🗆 X
mks_Vır	Repozyto	admin@127.0.0.1 25/0/4000 rium: 2024.05.29 10:09:33	Q 🚣 🏟 🚱
Zarządzane stacje	STACJA1 STACJA1 stacja ustawienia rapo	tester Windows 1	0 Pro ortv o infekciach z ostatnich 30 dni
	Data	Zdarzopio	Status
	2025 02 12 12:20:45	Skapowapia foldorów i plików	Infokcio
	2025-03-13 12:38:45	Skanowanie folderów i plików	Infekcja
	2025-03-13 12:38:08	Monitor under steedium objekt	Intekcja
	2025-03-13 12:33:32	Monitor wykrył szkodliwy obiekt	Intercja
	2025-03-13 12:33:20	Monitor wykrył szkodliwy obiekt	Infekcja
	2025-03-13 12:33:05	Monitor wykrył szkodiwy obiekt	Intekcja
	2025-03-13 12:32:55	Monitor wykrył szkodliwy obiekt	Infekcja
	2025-03-13 12:32:47	Monitor wykrył szkodiwy obiekt	Infekcja
	2025-03-13 12:30:35	Monitor wykrył szkodiwy obiekt	Intercja
	2025-03-13 12:30:16	Monitor wykrył szkodliwy obiekt	Intekcja
	2025-03-13 11:52:22	Monitor wykrył szkodiiwy obiekt	Infekcja
	2025-03-13 11:52:22	Monitor wykrył szkodiwy obiekt	Intekcja
	2025-03-13 11:52:18	Monitor wykrył szkodiwy obiekt	Intekcja
	2025-03-11 08:25:06	Monitor wykrył szkodiwy obiekt	Intekcja
	2025-03-11 08:24:57	Monitor wykrył szkodiiwy obiekt	Infekcja
	2025-03-11 08:24:47	Monitor wykrył szkodiiwy obiekt	Infekcja
	2025-03-11 08:24:39	Monitor wykrył szkodliwy oblekt	Intekcja
			incigu
			Wróć do domyślnego widoku raportów

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

m mks_vir - histori	a przeglądanych stron		-		×
Historia przeglą	danych stron z dnia: 2020.12.17	💙 Pokaż 🛛	wszys	tkie ad	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				-		>
tywność sieciowa z dnia	a: 2025.04.17	Dane lokalizacyjne	dostarcza ᠙	IPinfo		
Filtry	08:25:44 msedge.exe	→ 18.66.233.111	443 💻		Poland	
Przepuszczone 285	08:25:44 msedge.exe	→ 18.66.233.111	443 🛑		Poland	
Zablokowane 🛛 🛛	08:25:44 msedge.exe	➔ 18.66.233.111	443		Poland	
	08:25:44 msedge.exe	→ 13.227.146.106	443		Poland	
Przychodzące 🗧 🏻	08:25:44 msedge.exe	→ 23.88.75.103	443 💻		Germany	1
🛾 Wychodzące 🔶 285	08:25:43 msedge.exe	➔ 151.101.1.229	443 📕		United	S
P v4 285	08:25:43 msedge.exe	→ 54.38.136.25	443		Poland	
	08:25:43 msedge.exe	→ 13.227.146.106	443 💼		Poland	
Aplikacio	08:25:43 msedge.exe	→ 34.36.214.49	443 📕		United	S
Арікасје	08:25:43 msedge.exe	♦ 84.17.61.32	443 🕨		Czechia	1
mousocoreworker.exe	08:25:43 msedge.exe	→ 2.20.32.236	443		Poland	
msedge.exe	08:25:43 msedge.exe	→ 13.227.146.71	443		Poland	
msedgewebview2.exe	08:25:43 msedge.exe	→ 13.227.146.71	443		Poland	
searchapp.exe	08:25:43 msedge.exe	→ 13.227.146.8	443		Poland	
smartscreen.exe	08:25:43 msedge.exe	→ 216.58.215.78	443 💼		Poland	
svchost.exe	08:25:43 msedge.exe	→ 20.79.107.10	443 💻		Germany	ŗ
systemsettings.exe	08:25:43 msedge.exe	→ 13.227.146.106	443 💼		Poland	
-,	08:25:43 msedge.exe	→ 178.239.128.20	443		Poland	
	08:25:42 msedge.exe	→ 13.227.146.31	443 💼		Poland	
	08:25:42 msedge.exe	→ 13.248.170.130	443		United	S
	08:25:42 msedge.exe	→ 75.2.119.157	443		United	S
	08:25:42 msedge.exe	→ 15.197.153.132	443 📕		United	s

- 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:

	admin@127.0.0.1 20/0/4000 Repozytorium: 2024.05.29 10:09:33 ACJA4 2 tester 1 ustawienia raporty oprogramowanie nowanie zainstalowane w systemie ktualizacje systemu Windows Aplikacja E dgge Update	Filtr: Producent Microsoft Corporation	Q 🕹 🛱	
	ACJA4 • Action tester • Action	Windows 11 Pro Filtr: Producent Microsoft Corporation	Wersja	
STACJA1 STACJA2 STACJA3 STACJA3 Oprogram SERWER *	ustawienia raporty oprogramowanie nowanie zainstalowane w systemie ktualizacje systemu Windows Aplikacja Edge	Filtr: Producent Microsoft Corporation	Wersja	
SERWER *	ktualizacje systemu Windows Aplikacja Edge Edge Update	Filtr: Producent Microsoft Corporation	Wersja	
Ukryjai     Wicrosoft     Microsoft     Microsoft     Microsoft     microsoft     microsoft     microsoft     microsoft     microsoft     microsoft	ktualizacje systemu Windows Aplikacja : Edge : Edge Update	Filtr: Producent Microsoft Corporation	Wersja	
Microsoft Microsoft Microsoft mks_vir Środowis	Aplikacja : Edge : Edge Update	Producent Microsoft Corporation	Wersja	
Microsoft Microsoft mks_vir Środowis	t Edge t Edge Update	Microsoft Corporation		
	: Update Health Tools :ko uruchomleniowe Microsoft Edge WebVlew2	Microsoft Corporation Microsoft Corporation Arcabit/mks_vir 2 Microsoft Corporation	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.):

mks_vir administrator									-		×
mks_Vır		R	adı : epozytoriu	min@127.0 22/0/4000 m: 2024.0!	.0.1 ) 5.29 10:0	9:33		C	λ 🕶	<b>\$</b> (	0
Zarządzane stacje	ST (gru	ACJE									
STACJA2	grupa	ustawienia	raporty	oprog	gramow	anie pod	sumowani	le			
🖵 STACJA3 🖵 STACJA4	Eks	portuj podsum	iowanle grup	y do pliku C	sV	□w	dok podst	awowy			
SERWER 🕇	Nazwa	IP	System	Procesor	Pamlęć	Użytkownicy	Wersja bazy	Abonament	Oczekujące aktualizacje	% Pamięć	Pr
	STACJA1	10.0.0.101	Windows 10 Pro 6.2 X64	Intel(R) Core (TM) I3- 7100 CPU @ 3.90GHz	3987	tester	2024- 05-29 09:03:21	217	2	55%	19
	STACJA2	10.0.0.102	Windows 7 Ultimate 6.1 X64 SP 1.0	Intel(R) Core (TM) I3- 4130 CPU @ 3.40GHz	3983	tester	2024- 05-29 09:03:21	217	0	28%	0!
	STACJA3	10.0.0.103	Windows 8.1 Pro 6.2 X86	Intel(R) Core (TM) I3 CPU 540 @ 3.07GHz	3447	tester	2024- 05-29 09:03:21	217	1	26%	0'
	STACJA4	10.0.0.104	Windows 11 Pro 6.2 X64	Intel(R) Core (TM) I3- 9100 CPU @ 3.60GHz	16246	tester	2024- 05-29 09:03:21	217	2	16%	0'
	<										7

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