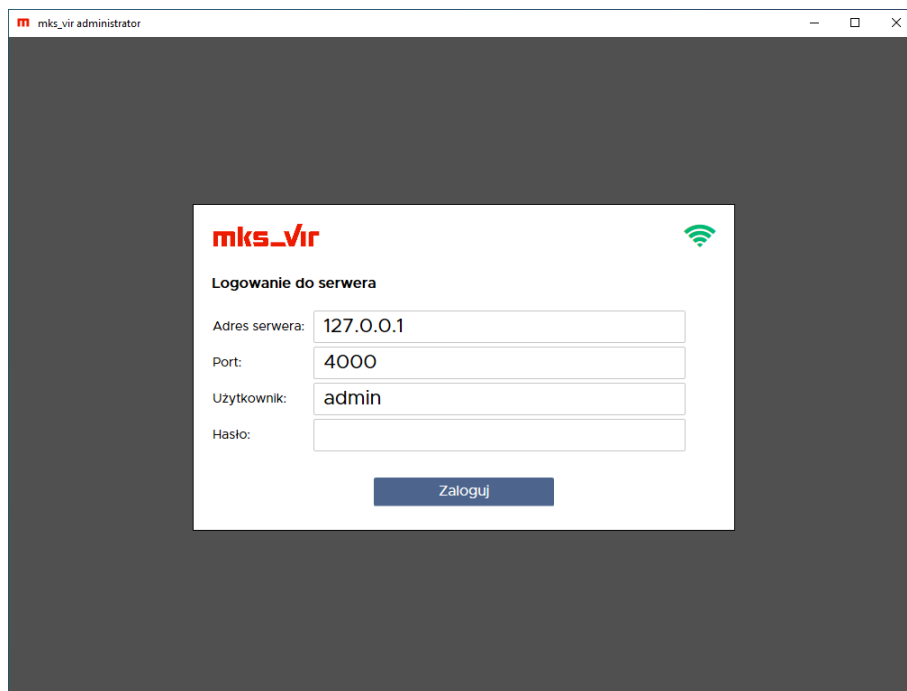


## mks\_vir administrator

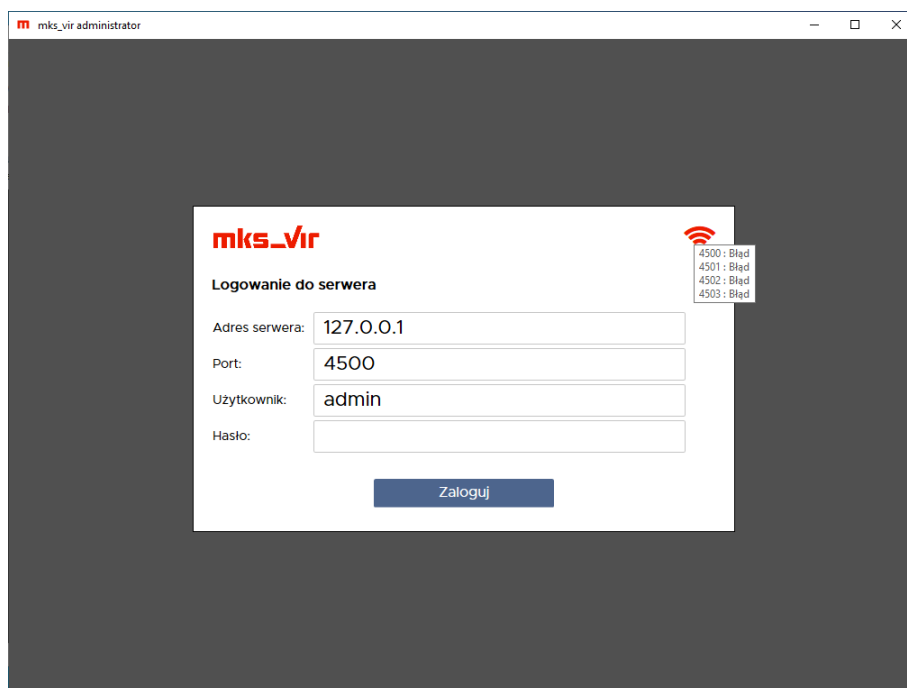
**mks\_vir administrator** służy do zarządzania instalacjami pakietów **mks\_vir** w sieci

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

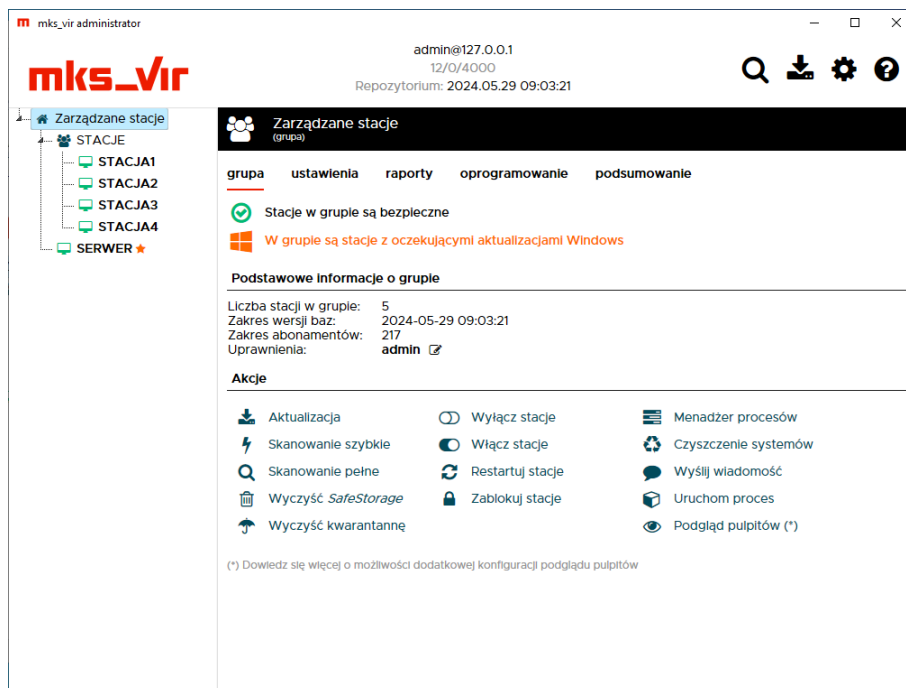
Jeśli serwer jest dostępny ikona ma kolor zielony 🟢:



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



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

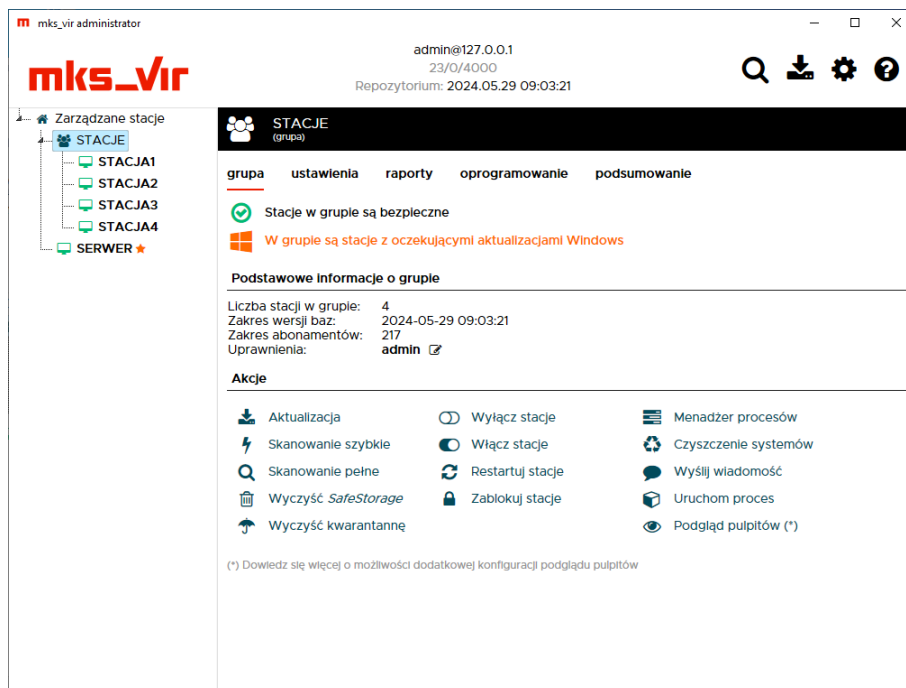


Jeśli jest widoczny napis „**W grupie są stacje z oczekującymi aktualizacjami Windows**”, to znaczy że na części stacji są oczekujące na instalację aktualizacje systemu Windows.

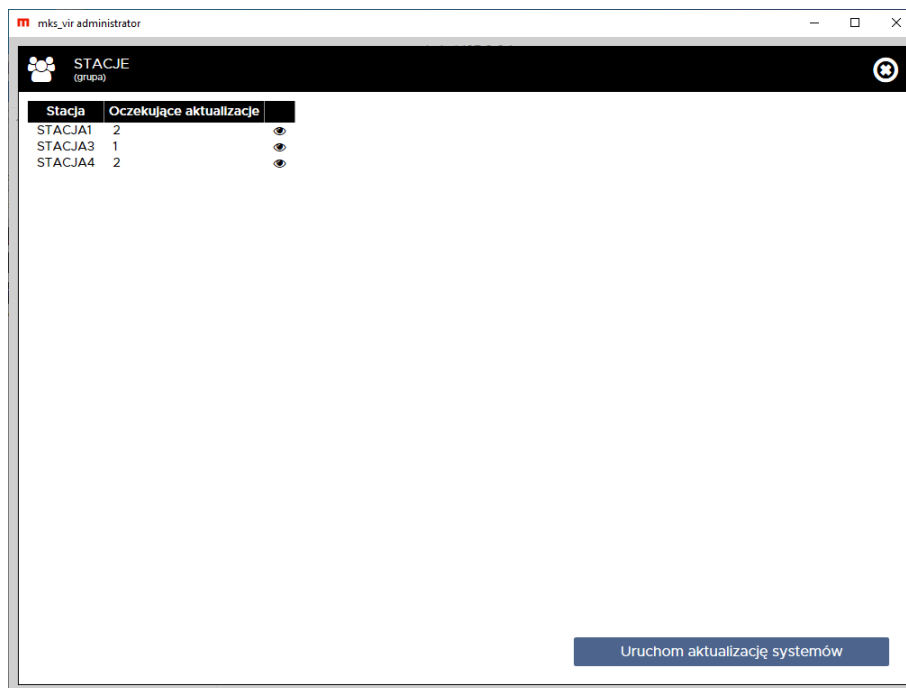
Ikony widoczne u góry okna konsoli, po prawej stronie, oznaczają:

- 🔍 – 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 🔍 zmieni się w ikonę ✕ – jej wciśnięcie zresetuje wyniki wyszukiwania
- ⬇️ – uruchomienie aktualizacji serwera zarządzającego **mks\_vir administrator** oraz repozytorium aktualizacyjnego dla stacji
- ⚙️ – ustawienia serwera zarządzającego i konsoli **mks\_vir administrator**
- ❓ – dostęp do podręcznika **mks\_vir**


## Podstawowe informacje o grupie:



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

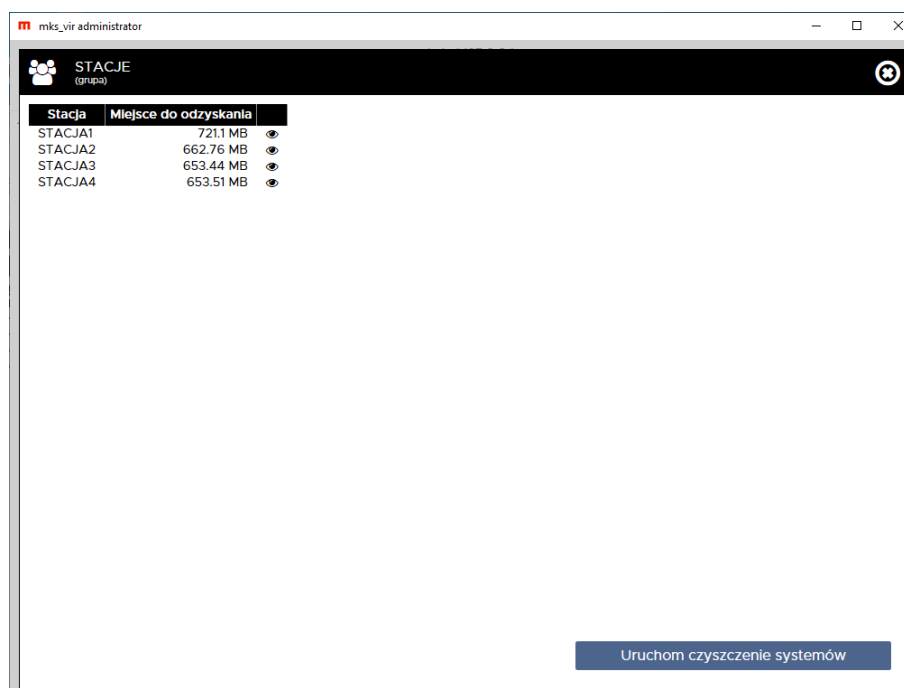


W linii „**Uprawnienia**” podane są informacje, którzy ze zdefiniowanych w ustawieniach konsoli i serwera zarządzającego użytkowników mają prawa dostępu do danej grupy (pozwalające na wyświetlanie i modyfikację parametrów danej grupy); użytkownik **admin** ma zawsze pełne uprawnienia do wszystkich grup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

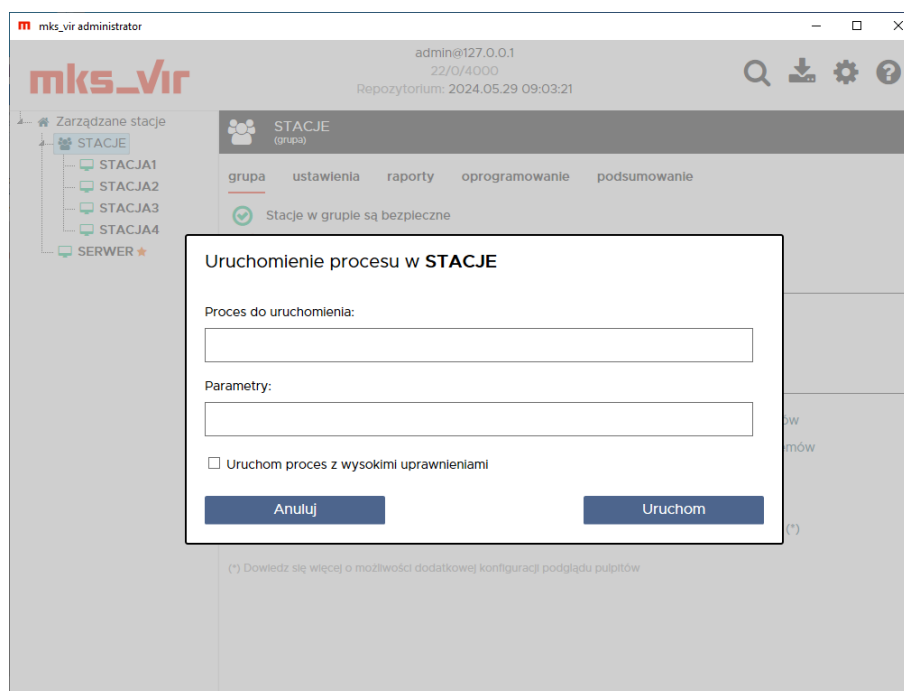
dostępu do grup dla innych zdefiniowanych użytkowników. Wybranie ikony  pozwala na modyfikację praw dostępu do danej grupy.

Przyciski dostępne w tej sekcji pozwalają na:

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

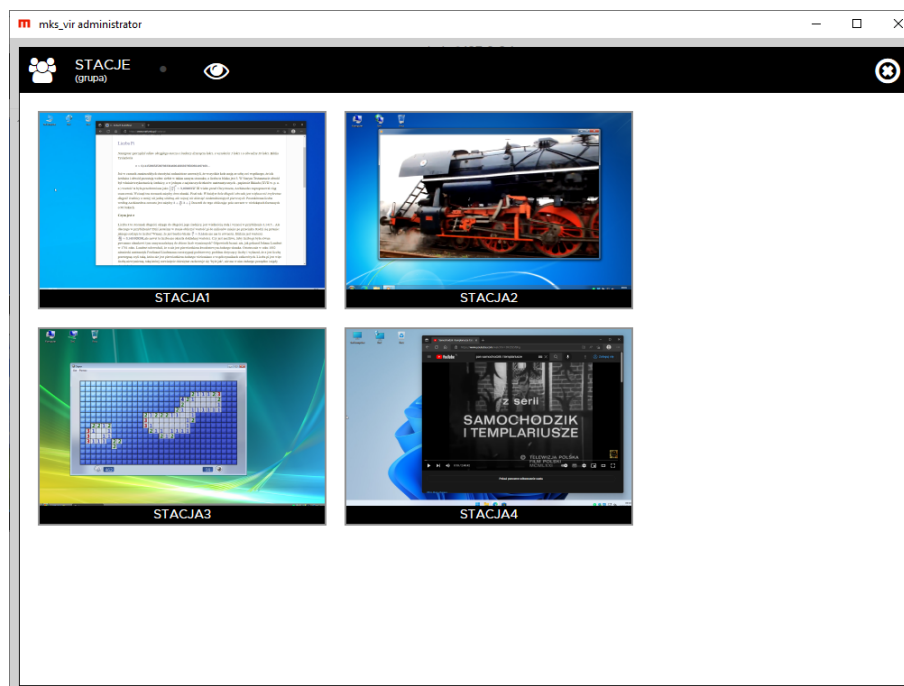


- **Wyślij wiadomość** – umożliwia wysłanie wiadomości do stacji w danej grupie
- **Uruchom proces** – pozwala na wysłanie do stacji w danej grupie polecenia uruchomienia jakiegoś programu:



gdzie:

- **Proces do uruchomienia** – tu podajemy nazwę pliku do uruchomienia, jeśli jest to konieczne razem ze ścieżką do tego pliku
  - **Parametry** – tu podajemy opcjonalne parametry wywołania procesu
  - **Uruchom proces z wysokimi uprawnieniami** – zaznaczenie opcji spowoduje uruchomienie procesu z uprawnieniami systemu, w przeciwnym razie proces będzie uruchomiony z uprawnieniami zalogowanego użytkownika
- **Podgląd pulpitów** – umożliwia wyświetlenie miniatur pulpitów stacji w danej grupie i podglądanie w czasie rzeczywistym działań użytkowników:



Kliknięcie w miniaturkę powoduje przeniesienie do sekcji danej stacji

## Podstawowe informacje o stacji:

admin@127.0.0.1  
21/0/4000  
Repozytorium: 2024.05.29 09:03:21

**mks\_vir**

Zarządzane stacje

- STACJE
  - STACJA1
  - STACJA2
  - STACJA3
  - STACJA4
  - SERWER ★

STACJA1 (stacja) | tester | Windows 10 Pro

stacja | ustawienia | raporty | oprogramowanie

Stacja jest bezpieczna

**Podstawowe informacje o stacji**

Nazwa stacji: TEST01 [09cd1307-6e1d-a880-31142113610f]  
 Adres: 10.0.0.101 [309c2341e24d]  
 Procesor: 1% Intel(R) Core(TM) i3-7100 CPU @ 3.90GHz  
 Pamięć: 56% 3987MB  
 Dyski: C: 118 GB 95 GB | Z: 931 GB 910 GB  
 Miejsce do odzyskania: 721.1 MB  
 Oczekujące aktualizacje: 2  
 Możliwy problem z dyskami: [Kliknij, żeby sprawdzić.](#)

**Pakiet mks\_vir**

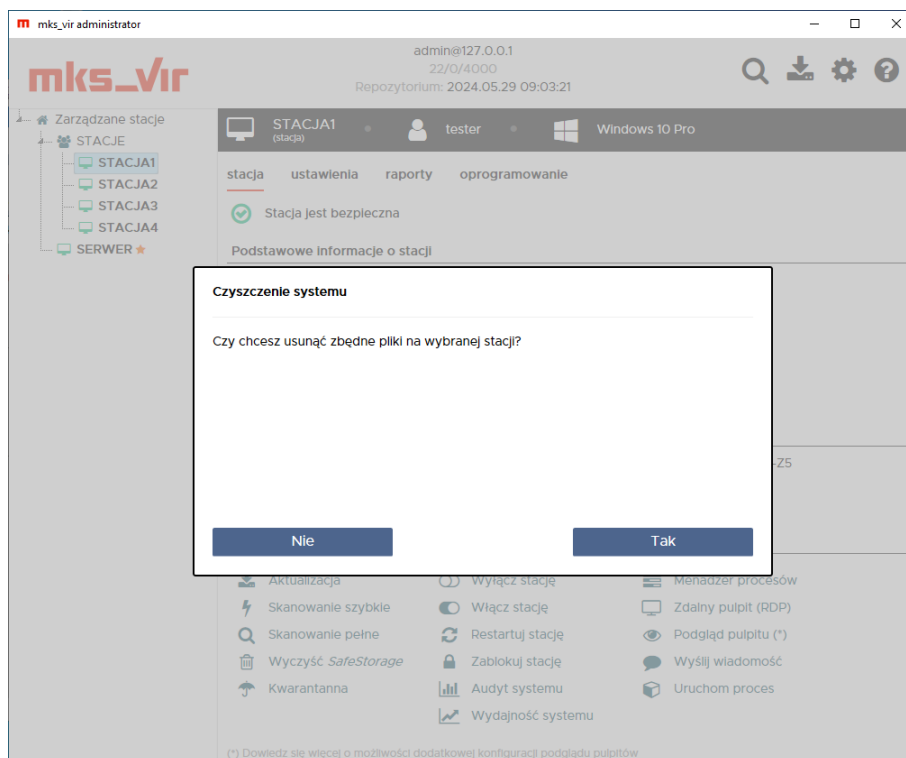
Numer licencji: TESTY-789B-BA94-A202-2011-OB0C-1087-D108-7F1E-10K1-G1H1-Z5  
 Licencja: 217  
 Wersja bazy: 2024-05-29 09:03:21  
 Dodatkowe informacje:

**Akcje**

- Aktualizacja
- Skanowanie szybkie
- Skanowanie pełne
- Wyczyść *SafeStorage*
- Kwarantanna
- Wyłącz stację
- Włącz stację
- Restartuj stację
- Zablokuj stację
- Audyt systemu
- Wydadajność systemu
- Menadżer procesów
- Zdalny pulpit (RDP)
- Podgląd pulpitu (\*)
- Wyślij wiadomość
- Uruchom proces

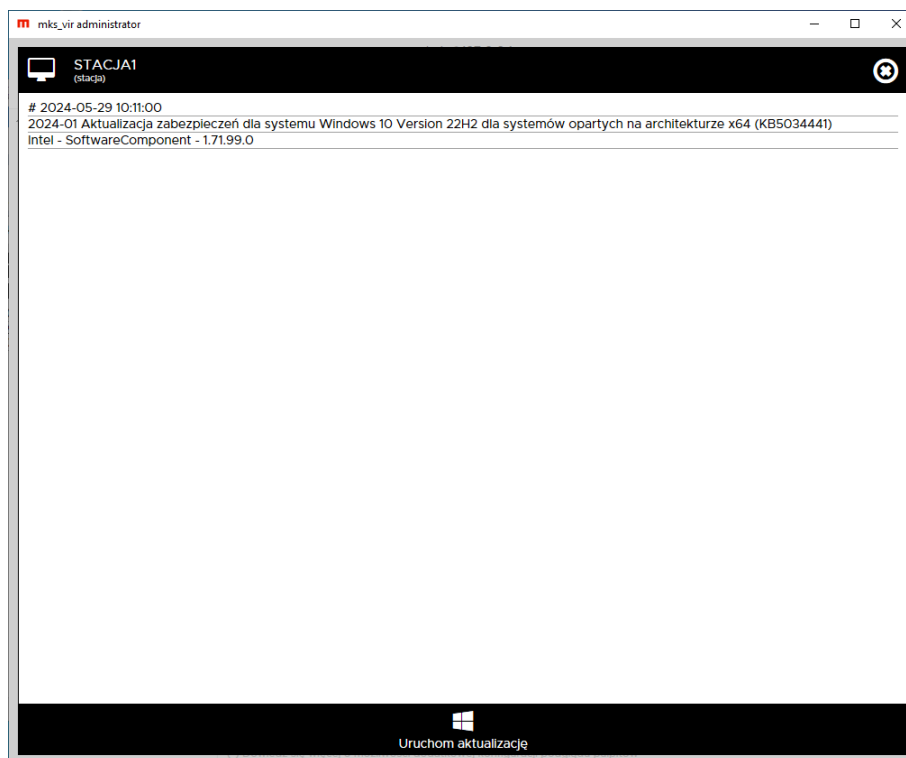
(\*) Dowiedz się więcej o możliwości dodatkowej konfiguracji podglądu pulpitu

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



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

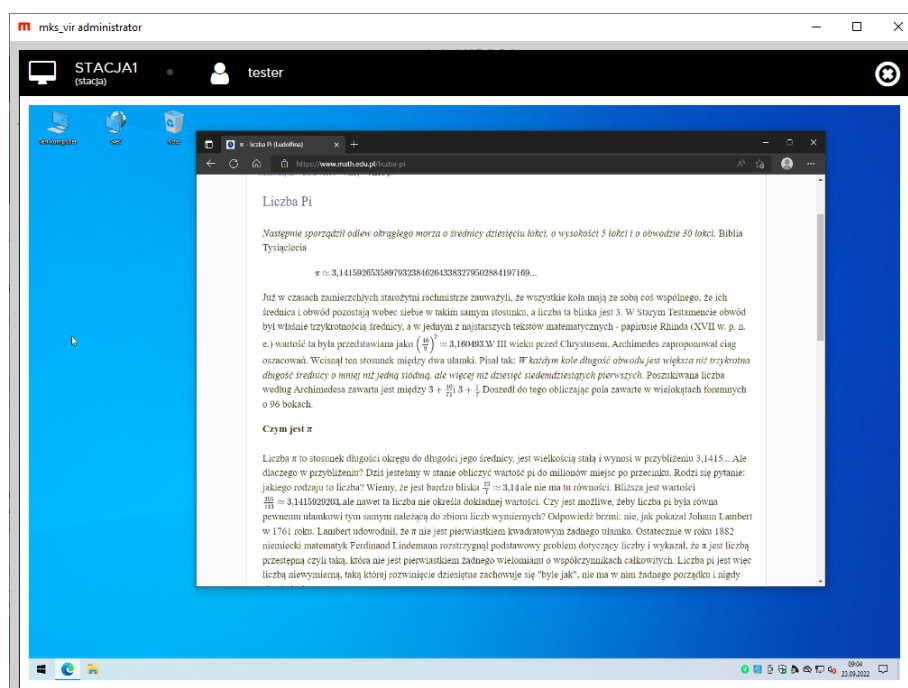
Jeśli jest widoczny napis „**Oczekujące aktualizacje**”, to znaczy że na tej stacji są oczekujące na instalację aktualizacje systemu Windows. Kliknięcie w ten napis powoduje wyświetlenie okna z listą oczekujących aktualizacji systemu Windows:



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

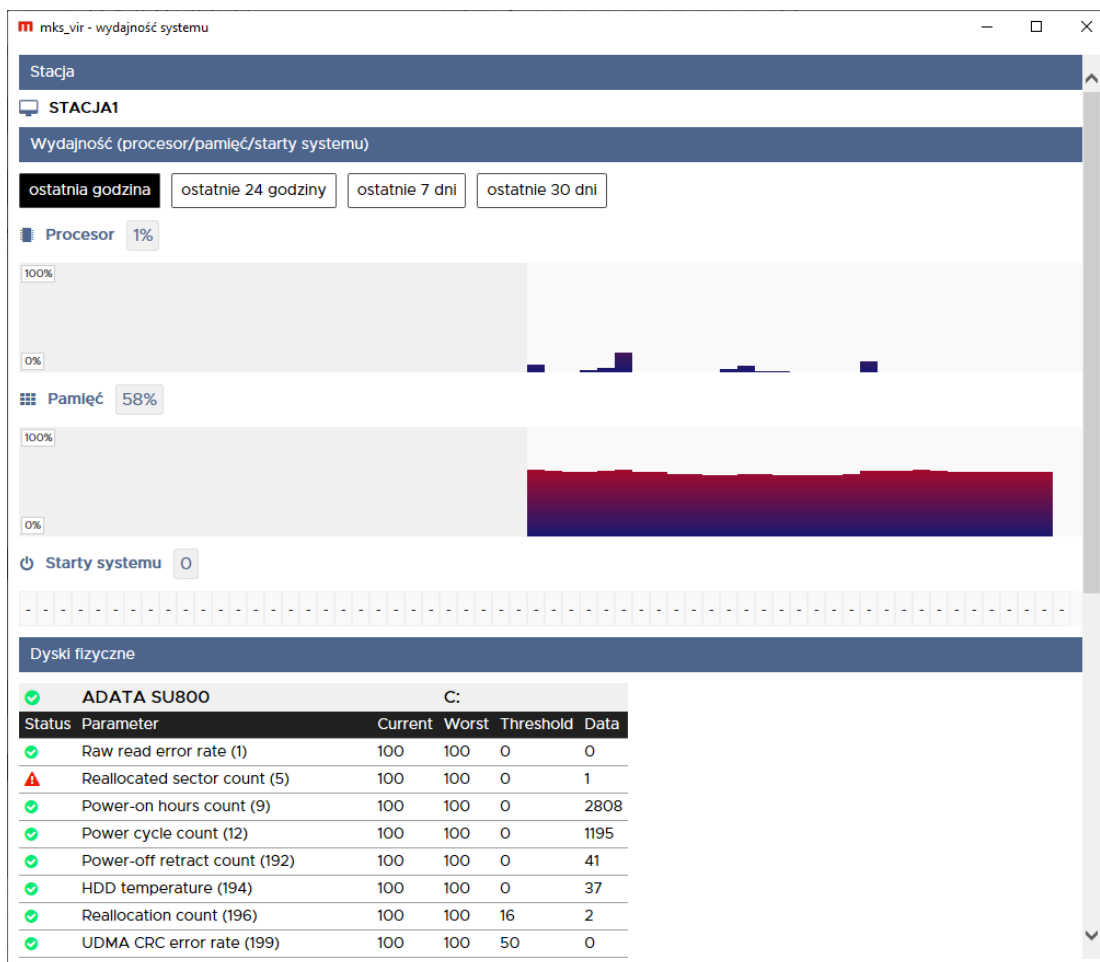
Przyciski dostępne w tej sekcji pozwalają na:

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





- **Wyślij wiadomość** – umożliwia wysłanie wiadomości do danej stacji
- **Wydajność systemu** – moduł pozwalający na ocenę parametrów pracy systemu i jego wydajności w zakresie ostatniej godziny, ostatniej doby (24 godziny) oraz ostatniego tygodnia (7 dni) i miesiąca (30 dni):



- **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

Zarządzane stacje (grupa)

grupa ustawienia **raporty** oprogramowanie podsumowanie

Aktywność modułów ochronnych

<input checked="" type="checkbox"/>	Ochrona plików	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Ochrona poczty	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Ochrona przeglądarki	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Zapora sieciowa (firewall)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Kontrola rodzicielska	<input type="checkbox"/>
<input type="checkbox"/>	Kontrola urządzeń USB	<input type="checkbox"/>
<input type="checkbox"/>	Kontrola urządzeń multimedialnych	<input type="checkbox"/>
<input type="checkbox"/>	Kontrola aplikacji	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Ochrona rejestru	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Ochrona w chmurze	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Ochrona RoundKick EDR	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Dostęp do Internetu	<input checked="" type="checkbox"/>

Ustawienia

[Pokaż szczegółowe ustawienia pakietu mks\\_vir](#)

Numer licencji

Grupa nie ma zdefiniowanego własnego numeru licencji [Zmień 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 (firewall)** – jeśli zapora będzie nieaktywna, to zmiana stanu **Dostępu do Internetu** nie będzie powodowała żadnych efektów. Aktywna blokada dostępu do sieci Internet na stacjach jest sygnalizowana zmienionym wyglądem ikony programu **mks\_vir** na

## Raporty:

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

admin@127.0.0.1  
22/0/4000  
Repozytorium: 2024.05.29 10:09:33

Zarządzane stacje (grupa)

grupa ustawienia **raporty** oprogramowanie podsumowanie

Statystyki grupy są wyliczane na podstawie raportów o wykrytych infekcjach z ostatnich 30 dni.

[Eksportuj wszystkie raporty grupy do pliku CSV](#)

TOP 10 wykrytych infekcji w grupie

Win32.Sality.OG	3	<div style="width: 30px; height: 10px; background-color: red;"></div>
EICAR-Test-File (not a virus)	2	<div style="width: 20px; height: 10px; background-color: red;"></div>
Trojan.A	1	<div style="width: 10px; height: 10px; background-color: red;"></div>
Trojan.Mikey.D23070	1	<div style="width: 10px; height: 10px; background-color: red;"></div>
Win32.Worm.Allaple.Gen	1	<div style="width: 10px; height: 10px; background-color: red;"></div>
Win32.Virtob.Gen.12	1	<div style="width: 10px; height: 10px; background-color: red;"></div>
Win32.Virtob.3.Gen	1	<div style="width: 10px; height: 10px; background-color: red;"></div>

TOP 10 stacji z wykrytymi infekcjami w grupie

STACJA1	5	<div style="width: 50px; height: 10px; background-color: red;"></div>
STACJA2	5	<div style="width: 50px; height: 10px; background-color: red;"></div>

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

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

The screenshot shows the mks\_vir administrator interface. The user is logged in as 'admin@127.0.0.1' with '25/0/4000' and 'Repozytorium: 2024.05.29 10:09:33'. The interface is for 'STACJA1 (stacja)' and the user is 'tester' on a 'Windows 10 Pro' system. The 'raporty' tab is active. A dropdown menu shows 'Raporty z dnia: 2025-03-17'. There are buttons for 'Pokaż historię przeglądanych stron' and 'Pokaż aktywność sieciową'. The table below shows the following data:

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

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

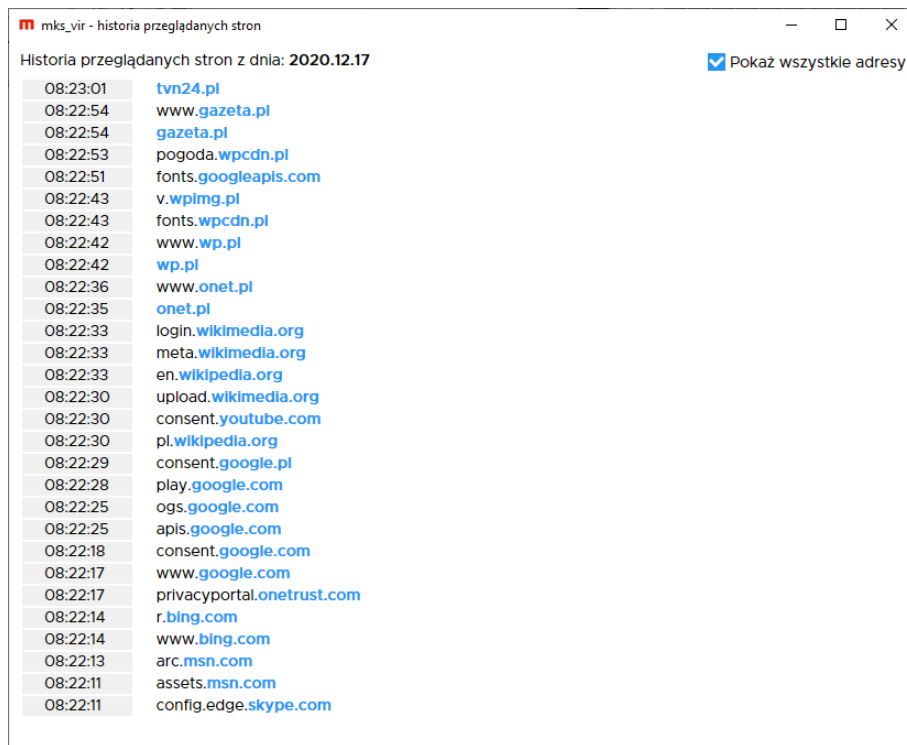
Po wybraniu „Pokaż tylko raporty o infekcjach” pojawią się tylko raporty z wykrytymi infekcjami w ostatnich 30 dniach; powrót do normalnego wyświetlania raportów jest możliwy przez wybranie „Wróć do domyślnego widoku raportów”:

The screenshot shows the mks\_vir administrator interface with the 'raporty o infekcjach z ostatnich 30 dni' view selected. The table below shows the following data:

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

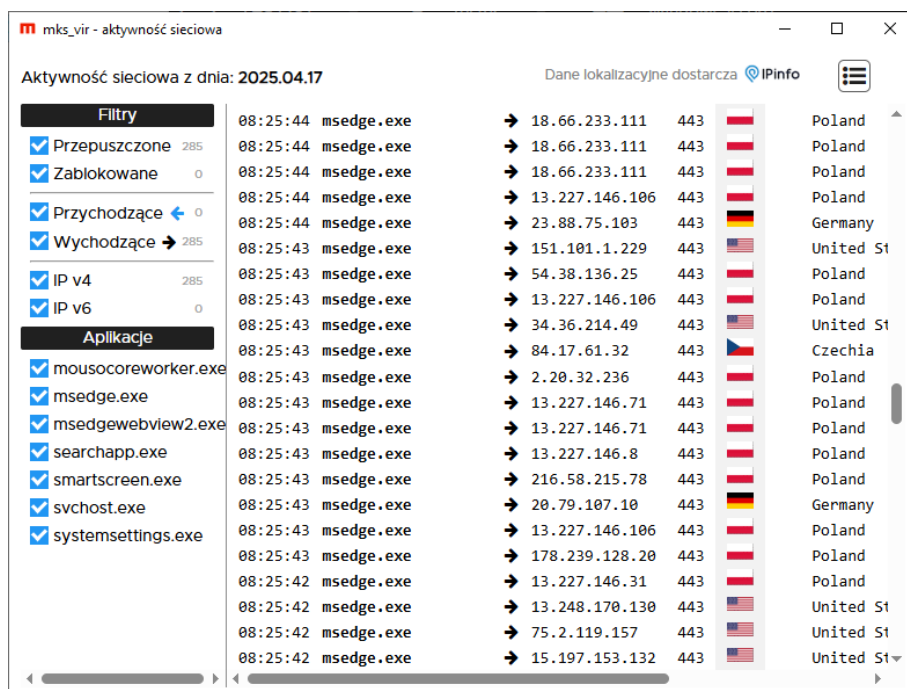
At the bottom right, there is a link: 'Wróć do domyślnego widoku raportów'.

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



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

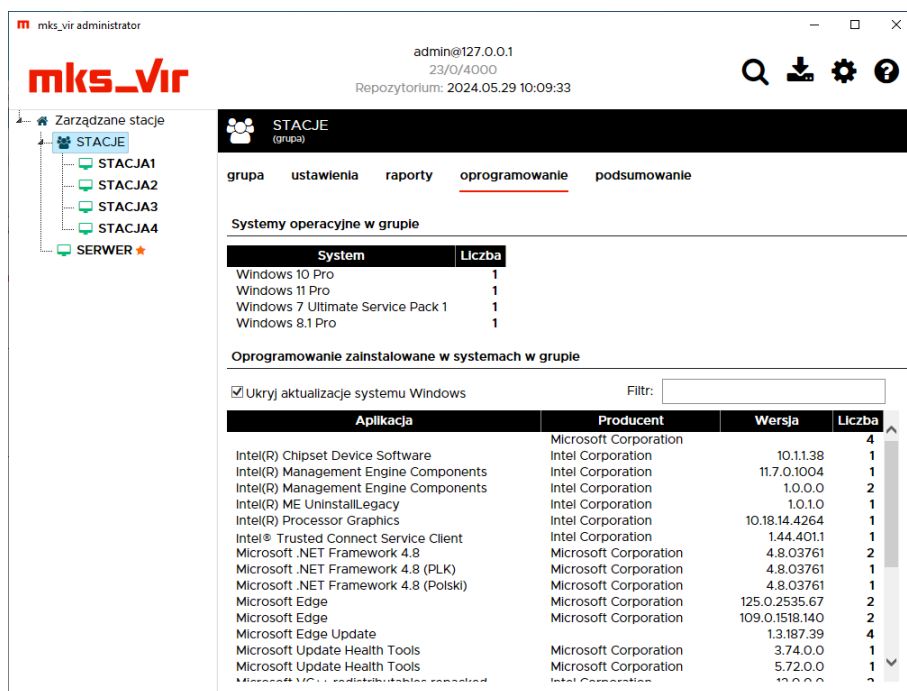
Po wybraniu „Pokaż aktywność sieciową” pojawi się okno pozwalające na przeglądanie aktywności sieciowej systemu i zainstalowanych aplikacji:



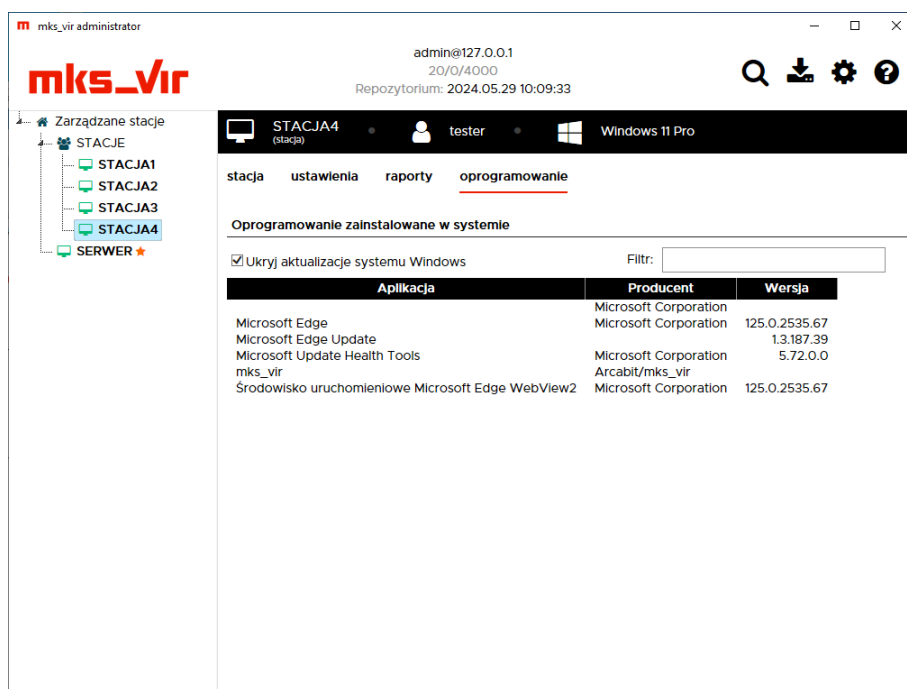
- **Filtry** – pozwala na filtrację aktywności:
  - dla połączeń przepuszczonych lub **zablokowanych**
  - dla połączeń przychodzących (←) lub wychodzących (→)
  - dla połączeń na protokołach **IP v4** lub **IP v6**
- **Aplikacje** – pozwala na filtrację aktywności połączeń dla określonych aplikacji

## Oprogramowanie:

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

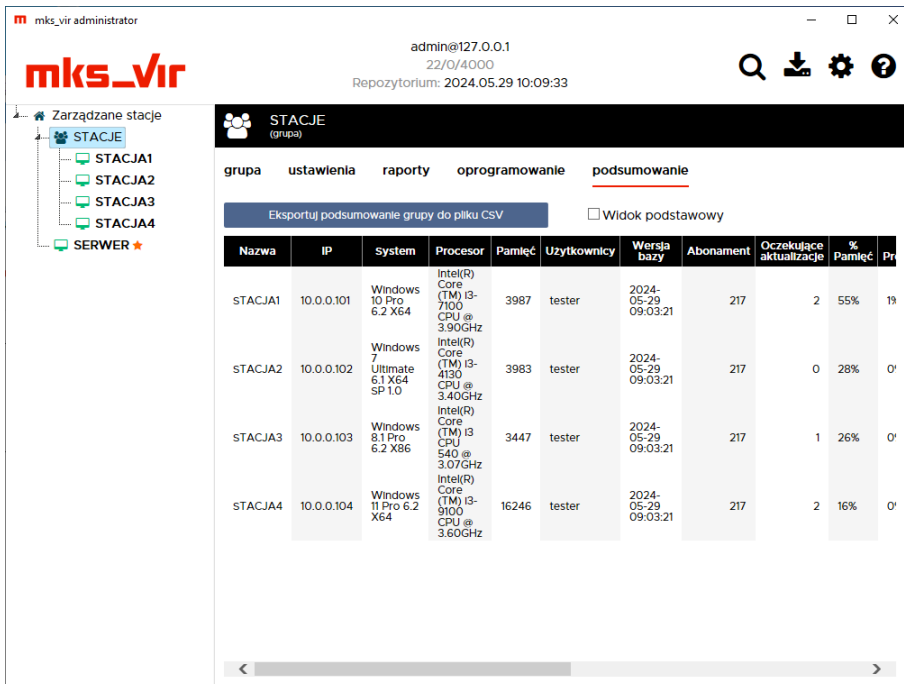


W przypadku stacji jest widoczna lista zainstalowanych na niej aplikacji:



## Podsumowanie:

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



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

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

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

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