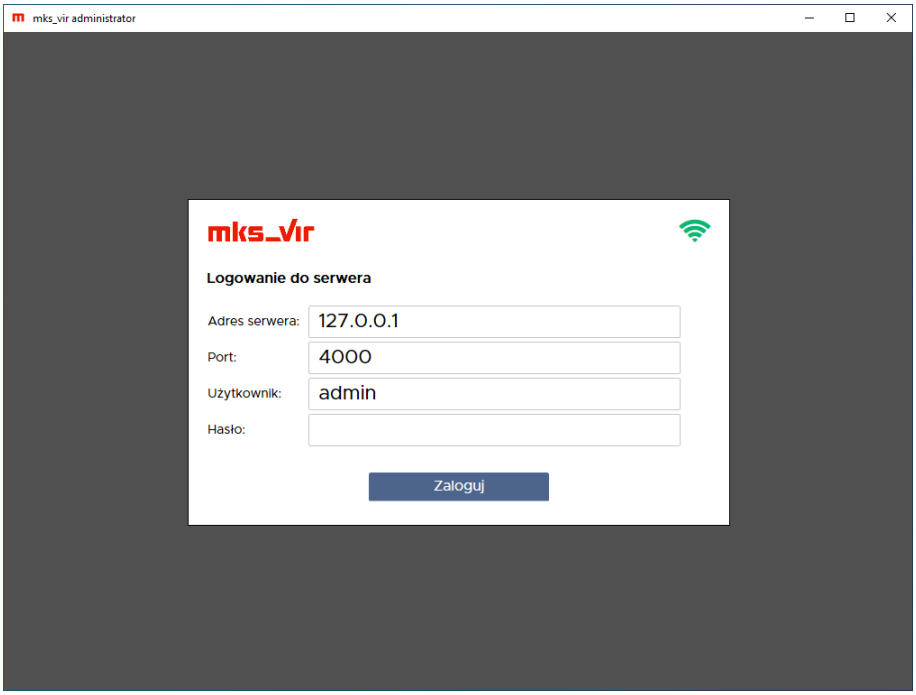
mks_vir administrator

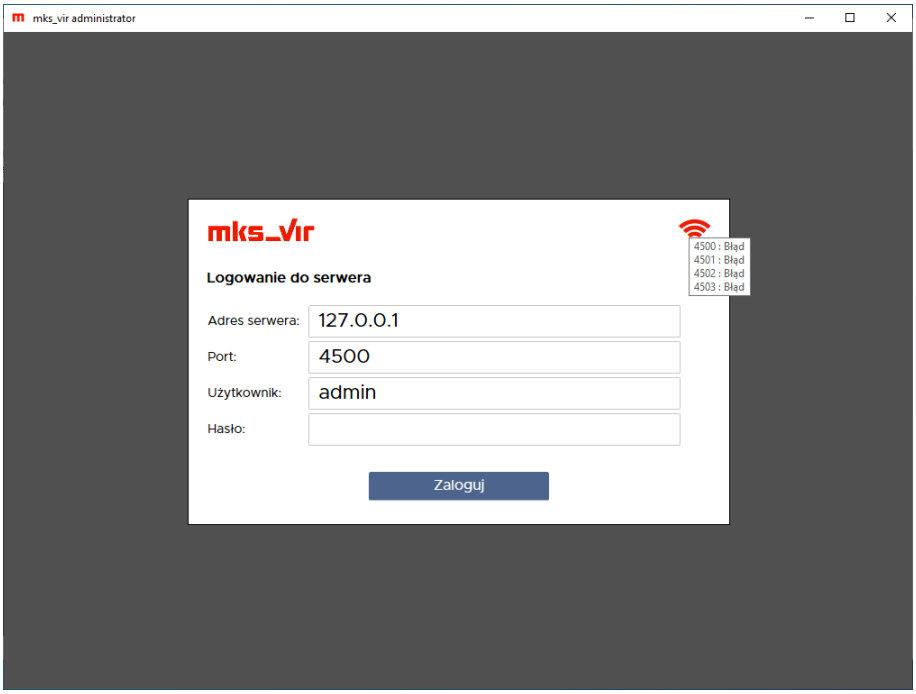
mks_vir administrator służy do zarządzania instalacjami pakietów **mks_vir** w sieci

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 .

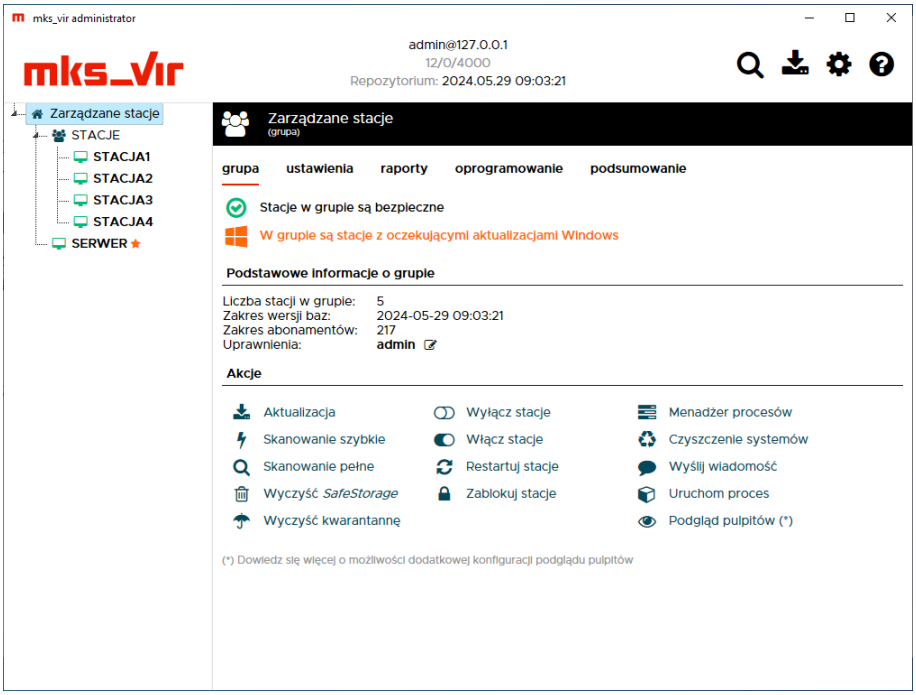
Jeśli serwer jest dostępny ikona ma kolor zielony :



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”)

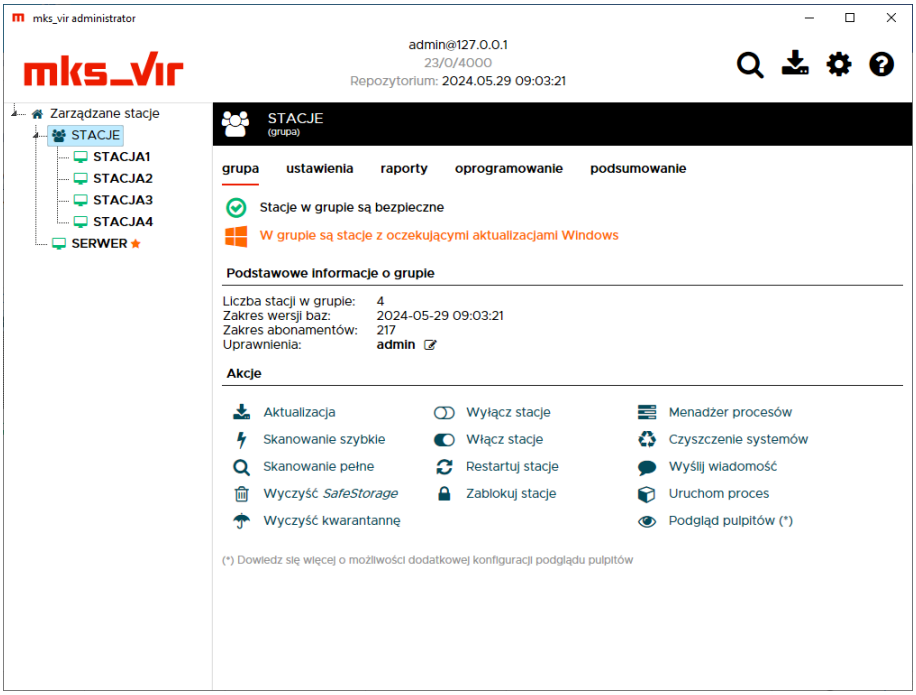
po wyszukaniu stacji ikona 🔍 zmieni się w ikonę ✖ – jej wciśnięcie zresetuje wyniki wyszukiwania

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

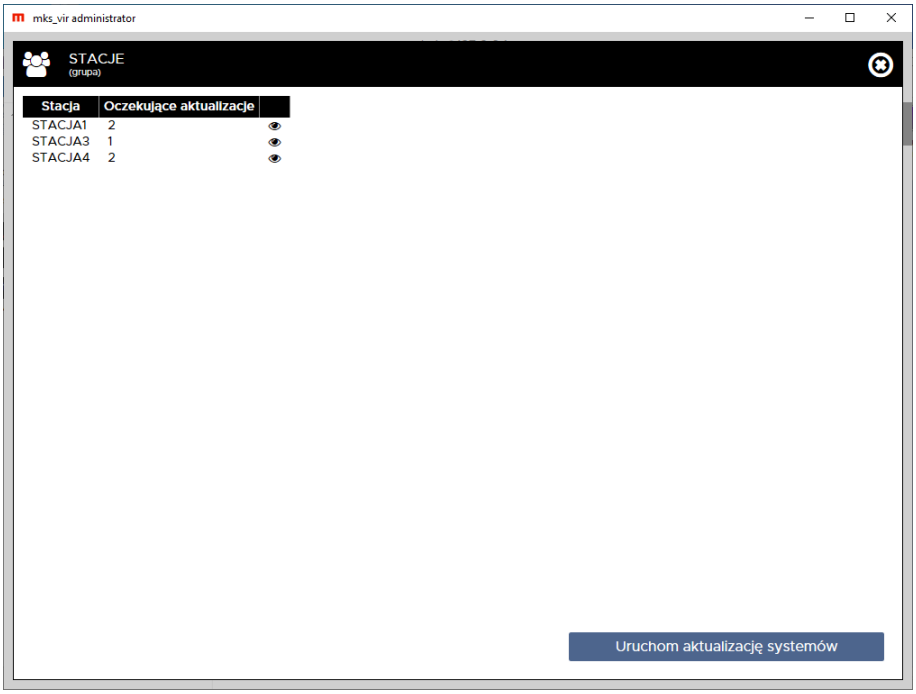
⚙ – ustawienia serwera zarządzającego i konsoli **mks_vir administrator**

❓ – 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:

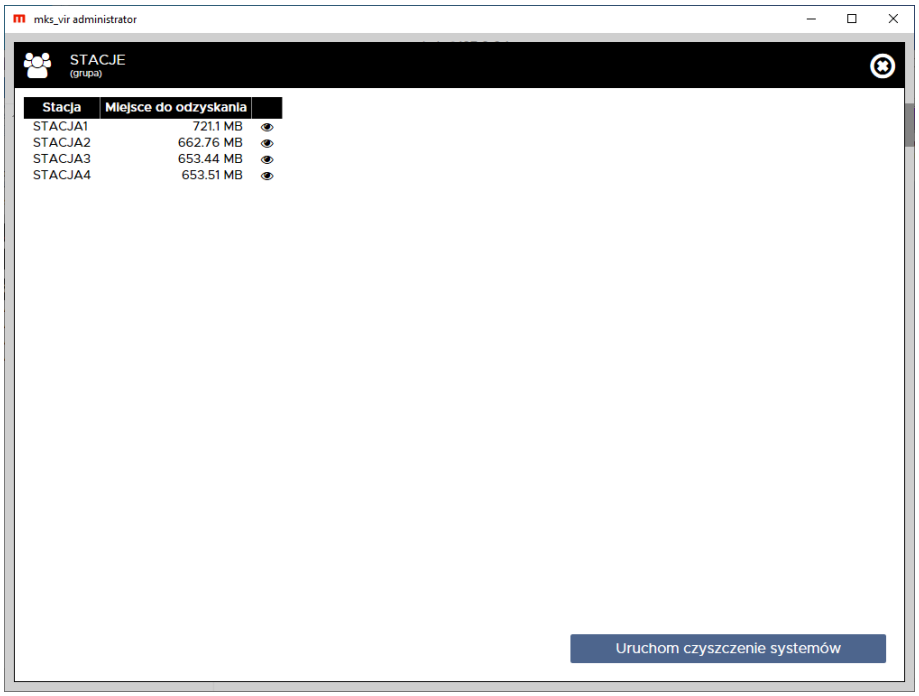


W linii **„Uprawnienia”** podane są informacje, którzy ze zdefiniowanych w ustawieniach konsoli i serwera zarządzającego użytkowników mają prawa dostępu do danej grupy (pozwalające na wyświetlanie i modyfikację parametrów danej grupy); użytkownik **admin** ma zawsze pełne uprawnienia do wszystkich grup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

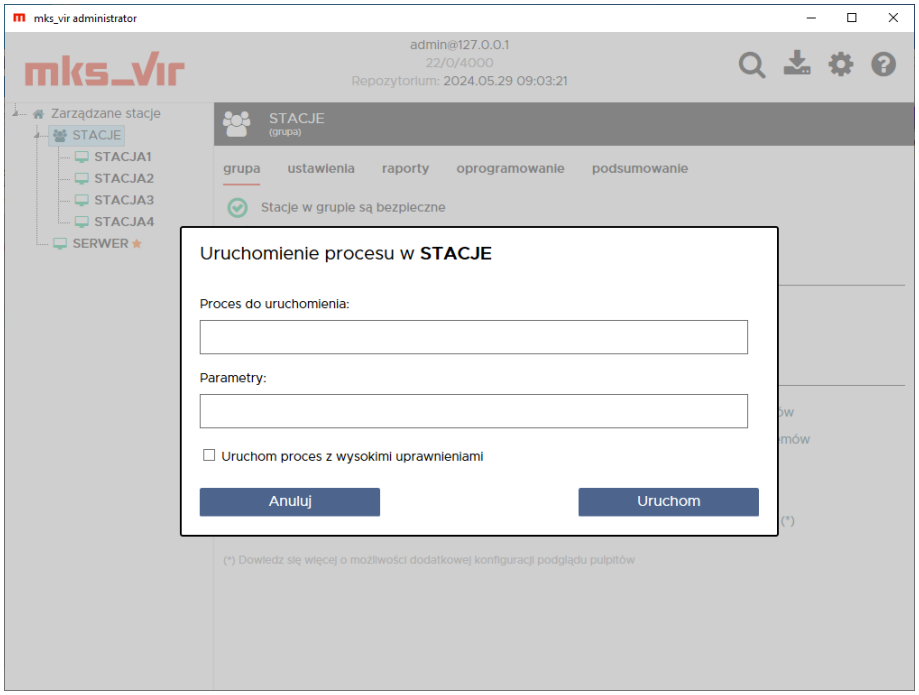
dostępu do grup dla innych zdefiniowanych użytkowników. Wybranie ikony pozwala na modyfikację praw dostępu do danej grupy.

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):



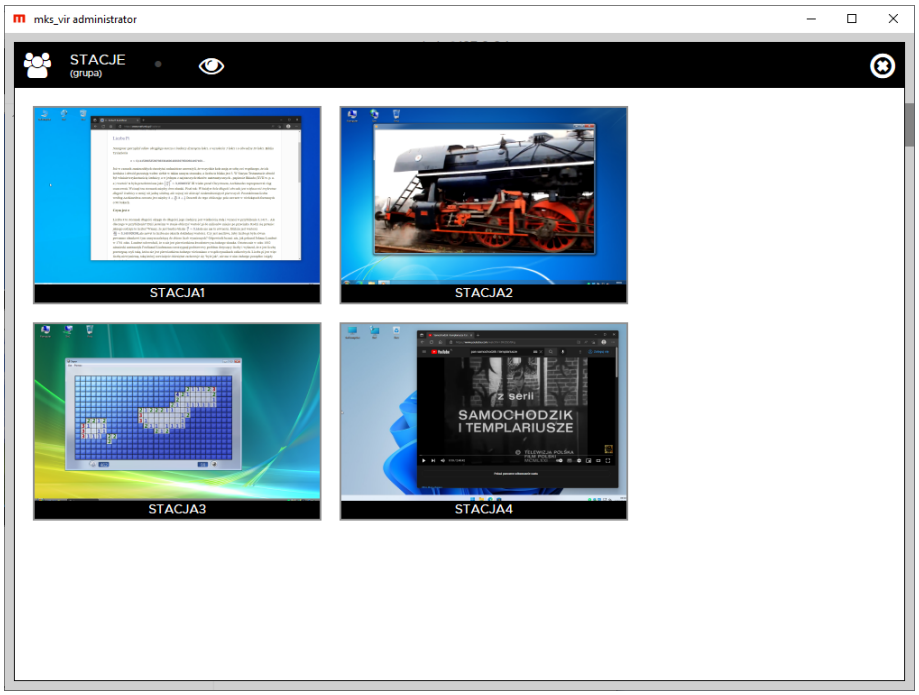
- **Wyślij wiadomość** – umożliwia wysłanie wiadomości do stacji w danej grupie
- **Uruchom proces** – pozwala na wysłanie do stacji w danej grupie polecenia uruchomienia jakiegoś programu:



gdzie:

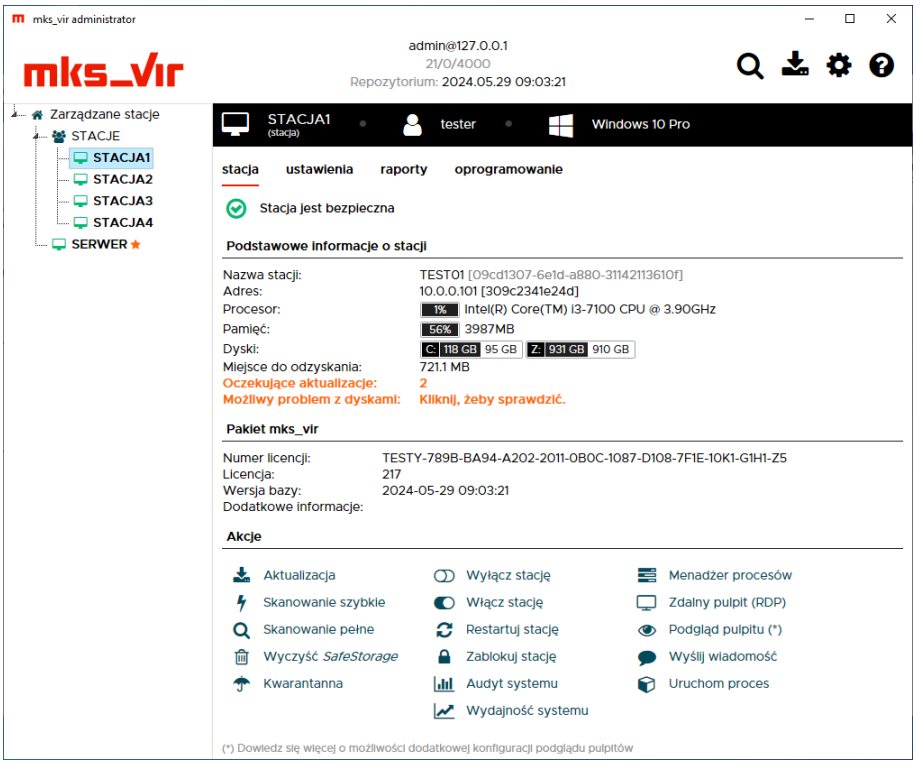
  - **Proces do uruchomienia** – tu podajemy nazwę pliku do uruchomienia, jeśli jest to konieczne razem ze ścieżką do do tego pliku
  - **Parametry** – tu podajemy opcjonalne parametry wywołania procesu
  - **Uruchom proces z wysokimi uprawnieniami** – zaznaczenie opcji spowoduje uruchomienie procesu z 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:

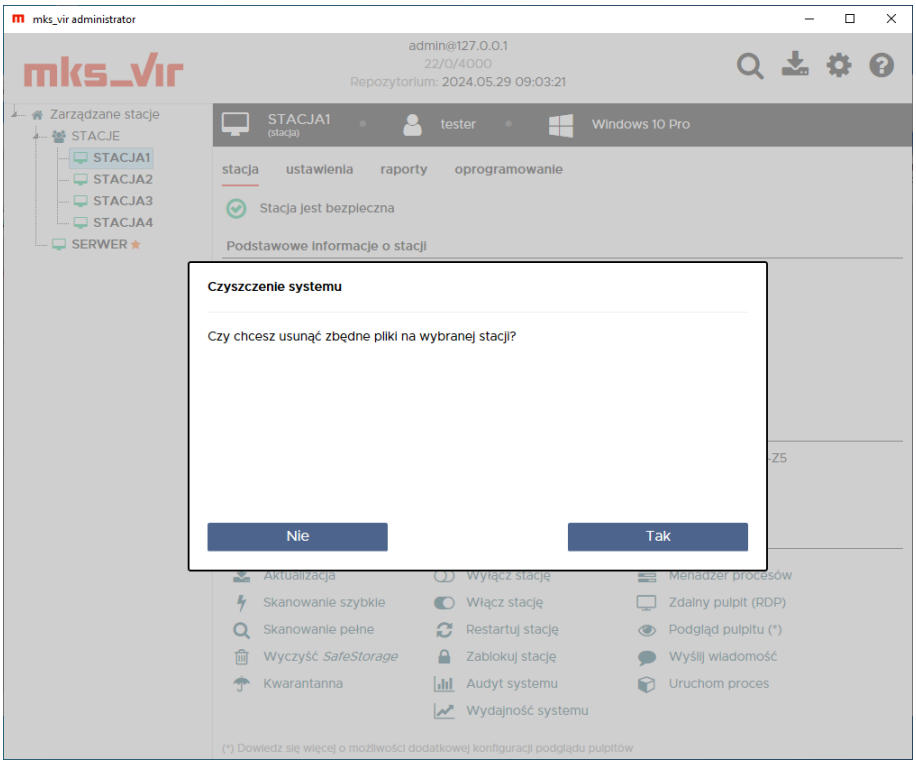


Kliknięcie w miniaturkę powoduje przeniesienie do sekcji danej stacji

Podstawowe informacje o stacji:

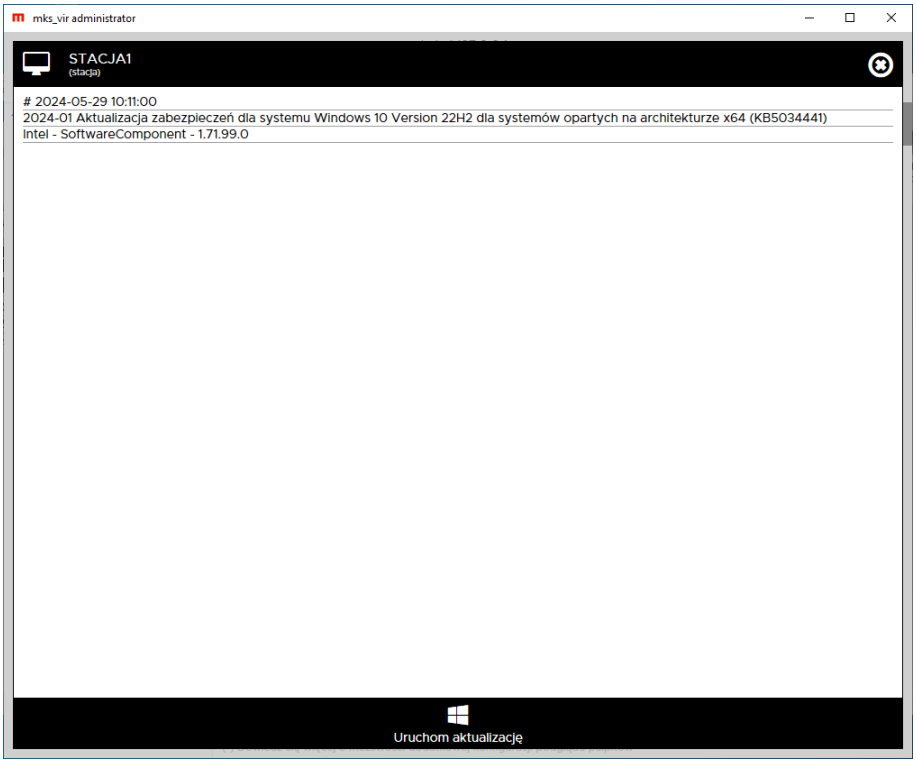


Jeśli jest widoczny napis **„Miejsce do odzyskania”** wraz z wielkością, to znaczy że na tej stacji można zwolnić na dysku tyle miejsca, ile wskazuje wyświetlana wielkość. Kliknięcie umożliwi rozpoczęcie czyszczenia (czyli usunięcie zbędnych śmieci):



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.

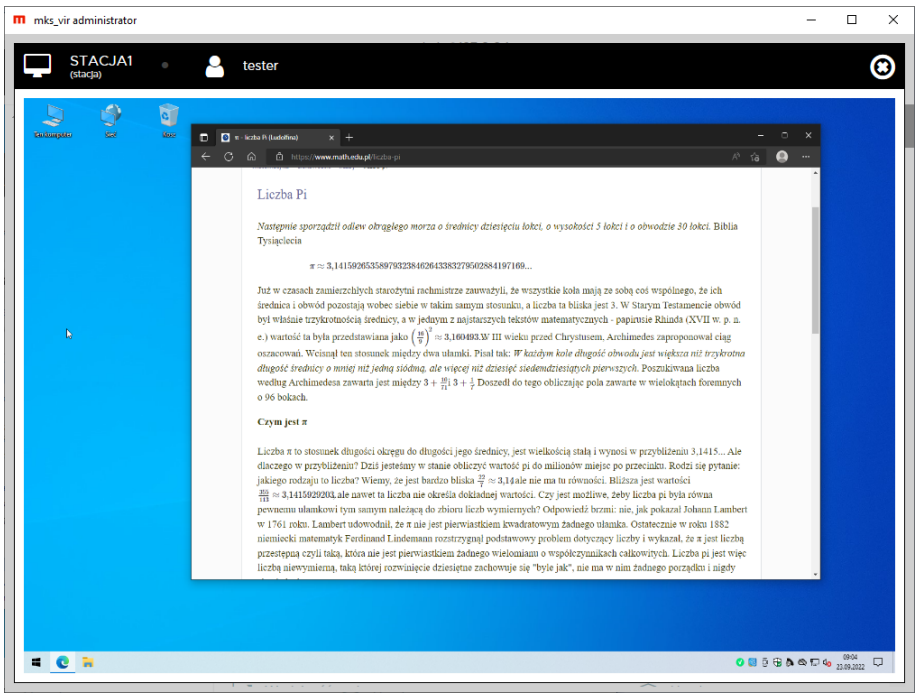
Jeśli jest widoczny napis **„Oczekujące aktualizacje”**, to znaczy że na tej stacji są oczekujące na instalację aktualizacje systemu Windows. Kliknięcie w ten napis powoduje wyświetlenie okna z listą oczekujących aktualizacji systemu Windows:



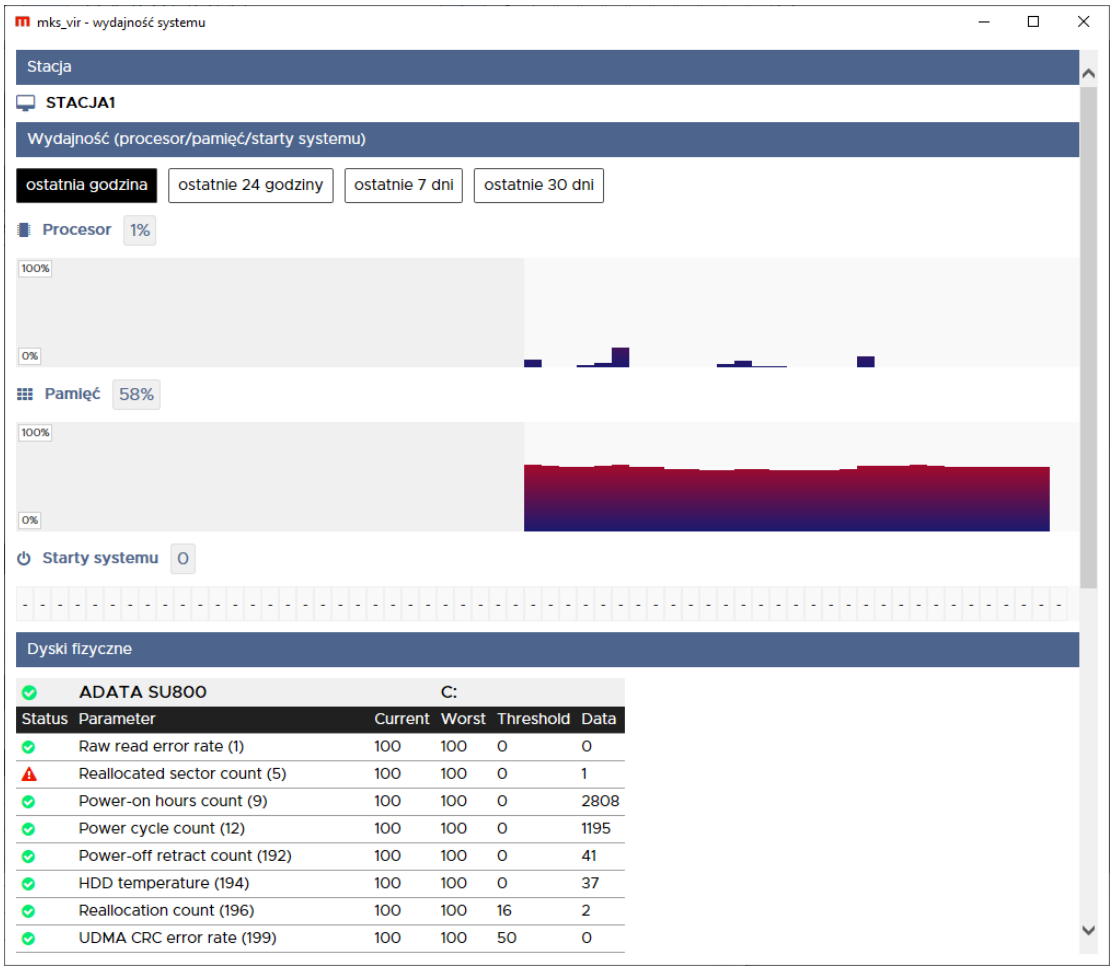
Wybranie **„Uruchom aktualizację”** powoduje wymuszenie instalacji oczekujących aktualizacji systemu Windows na danej stacji.

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
- **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):



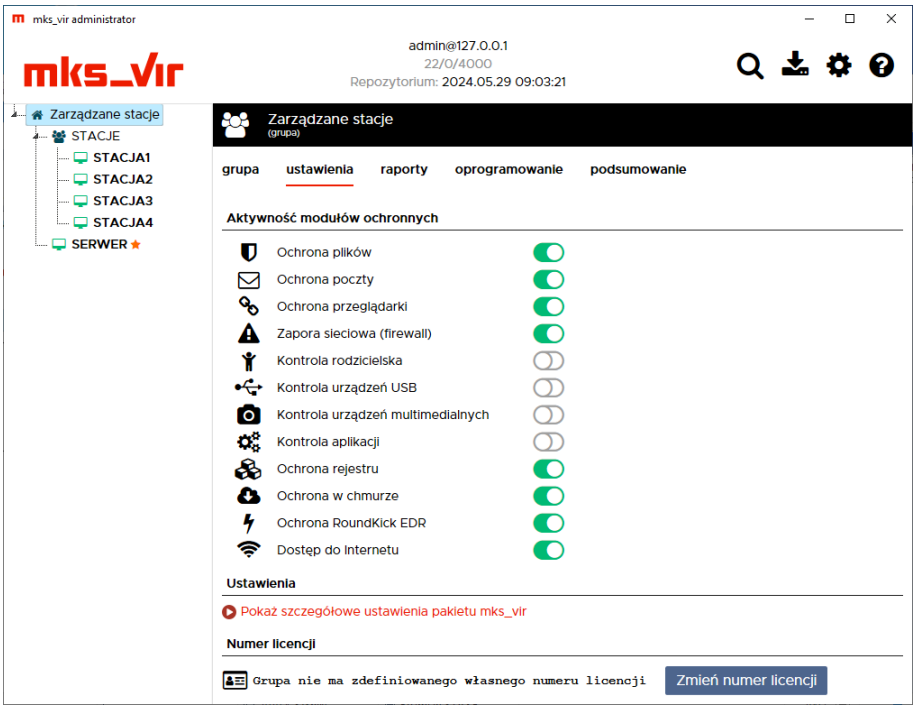
- **Uruchom proces** – pozwala na wysłanie do stacji polecenia uruchomienia jakiegoś programu

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

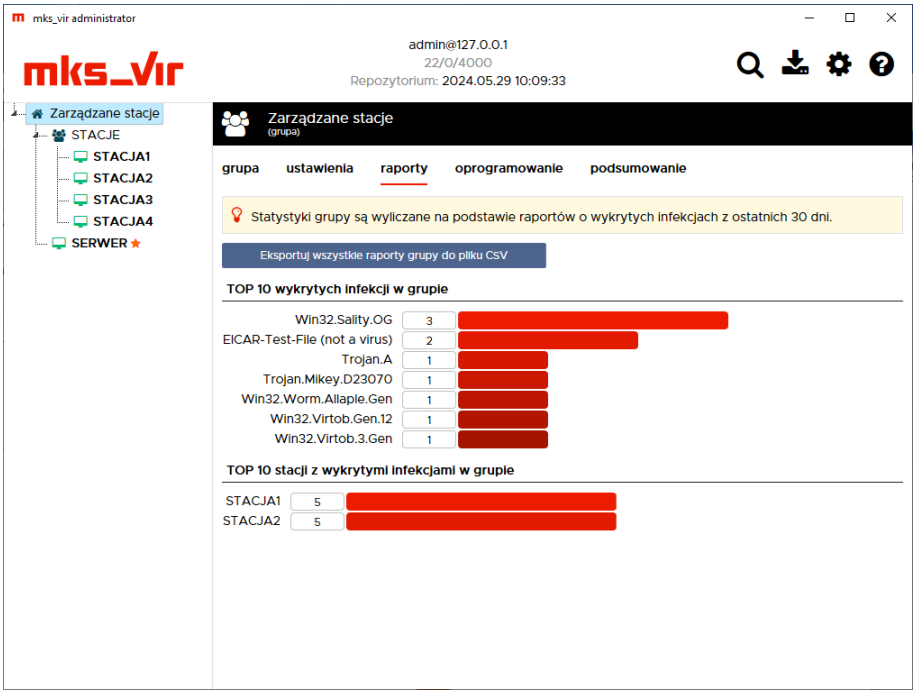
Jeżeli w danym elemencie (grupie lub stacji) nie ma zdefiniowanego numeru licencji, to stacje pracują na podstawie numeru licencji podanego przy ich instalacji



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

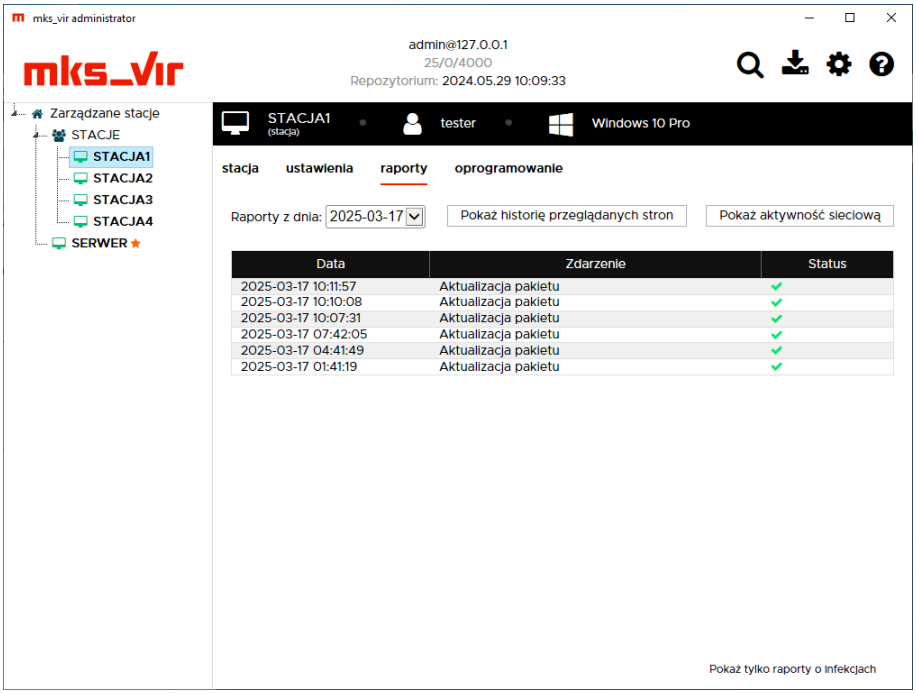
Raporty:

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

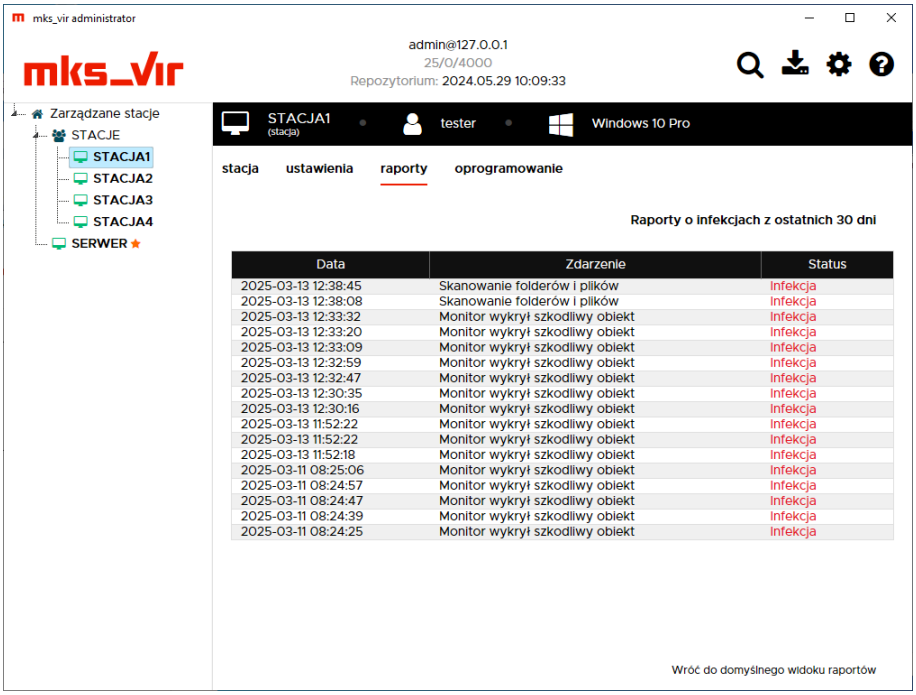


Możliwe jest też zapisanie wszystkich raportów grupy do pliku tekstowego w formacie CSV (potem można taki plik przetwarzać np. w Microsoft Excel, LibreOffice Calc itp.) za pomocą przycisku „*Eksportuj wszystkie raporty grupy do pliku CSV*”

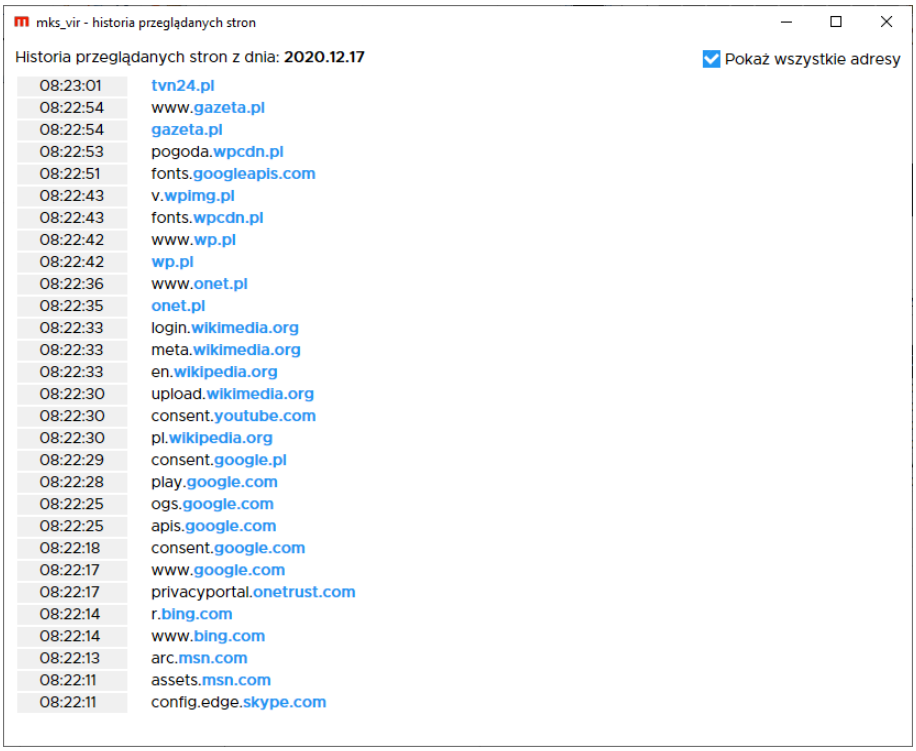
W przypadku stacji jest to tabela z widocznymi w niej poszczególnymi raportami z aktywności programu:



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*”:

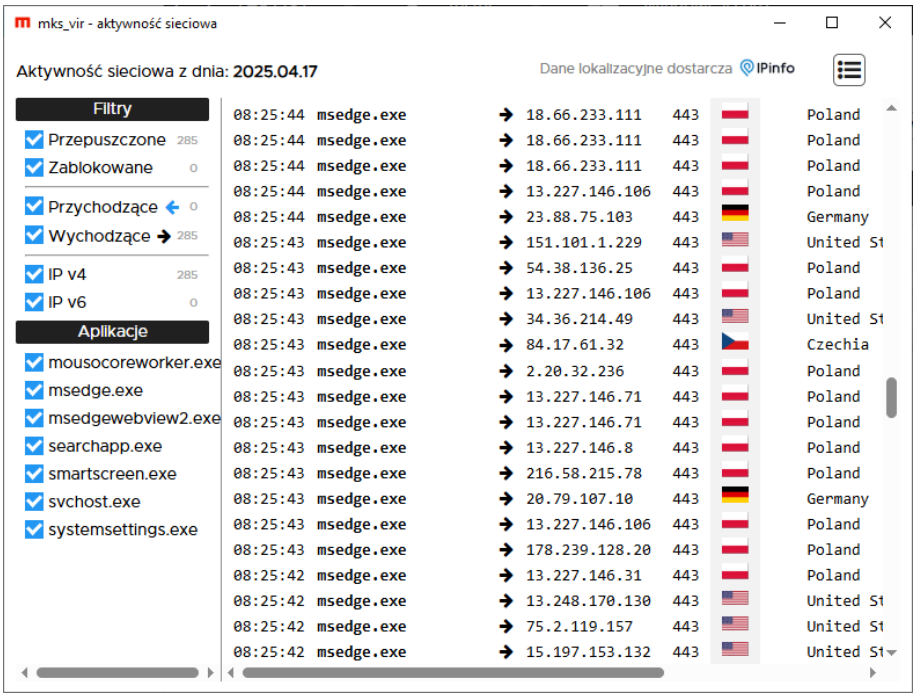


Po wybraniu „*Pokaż historię przeglądanych stron*” pojawi się okno pozwalające na przeglądanie aktywności internetowej użytkowników danej stacji:



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

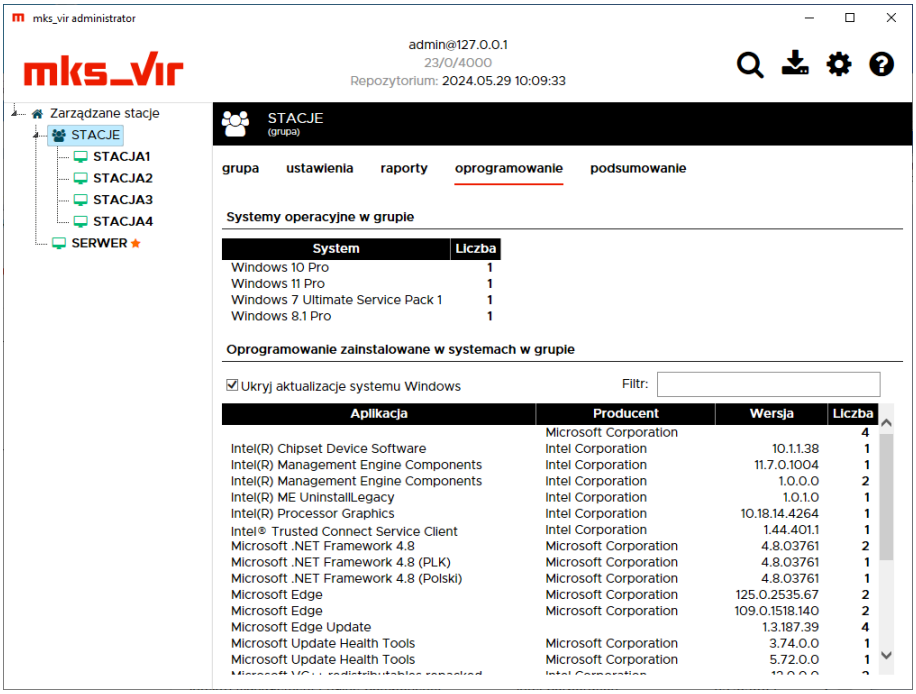
Po wybraniu „*Pokaż aktywność sieciową*” pojawi się okno pozwalające na przeglądanie aktywności sieciowej systemu i zainstalowanych aplikacji:



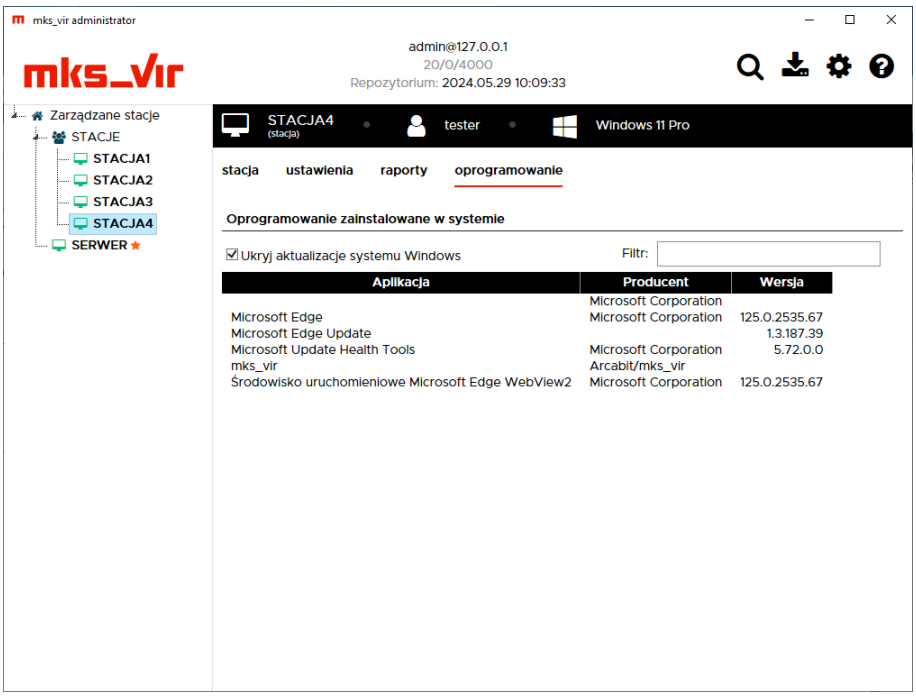
- **Filtry** – pozwala na filtrację aktywności:
  - dla połączeń przepuszczonych lub zablokowanych
  - dla połączeń przychodzących (←) lub wychodzących (→)
  - dla połączeń na protokołach **IP v4** lub **IP v6**
- **Aplikacje** – pozwala na filtrację aktywności połączeń dla określonych aplikacji

Oprogramowanie:

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

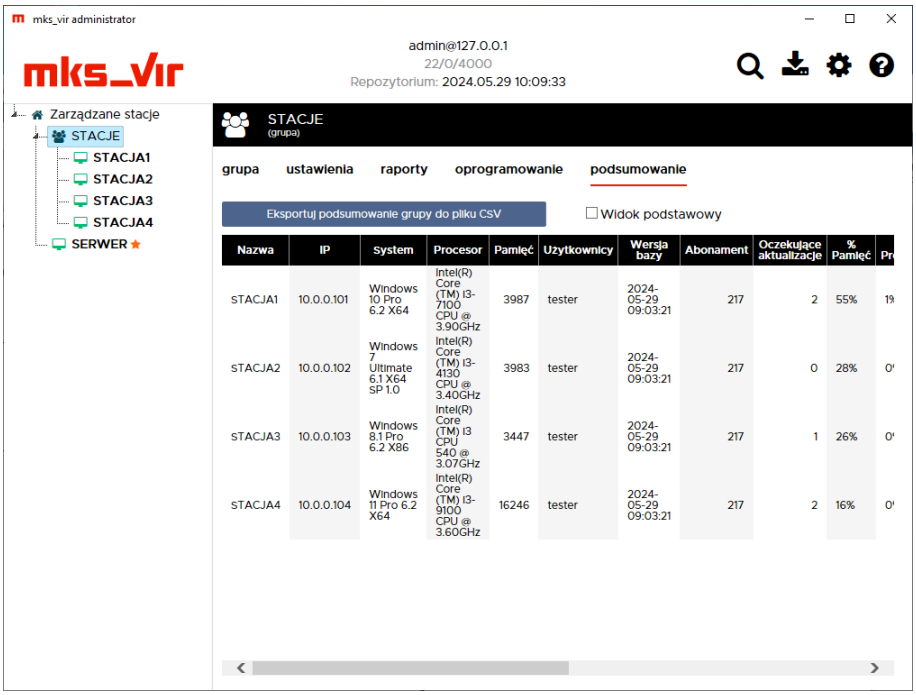


W przypadku stacji jest widoczna lista zainstalowanych na niej aplikacji:



Podsumowanie:

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



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