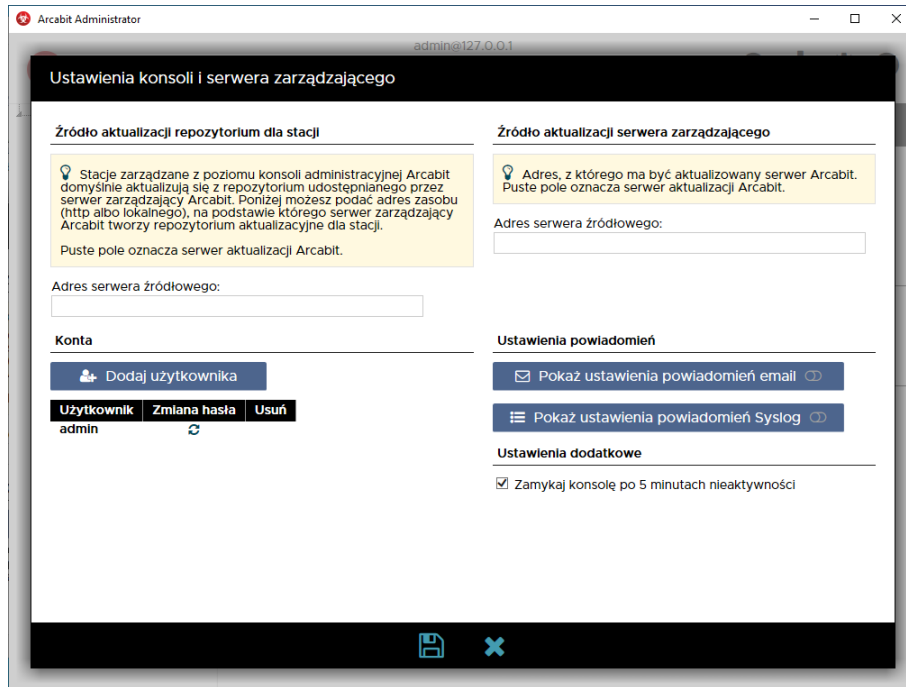
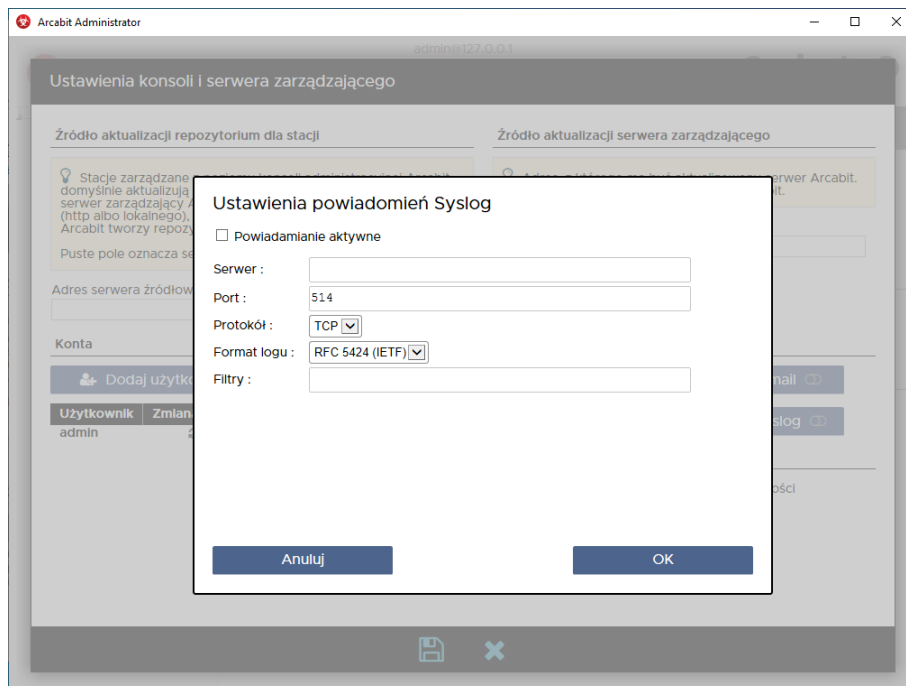


Arcabit Administrator – ustawianie powiadomień syslog

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



Uruchomi się okno konfiguracji powiadomień:



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

- **Serwer** – adres wykorzystywanego serwera SYSLOG

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



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



- **Filtry** – definicje rodzajów wysyłanych powiadomień

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

poniżej lista dopuszczalnych kodów:

- 0100 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **Arcabit**
- 0101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **Arcabit**
- 0103 – wysłanie powiadomienia w przypadku aktualizacji programu **Arcabit** odrzuconej przez użytkownika
- 0301 – wysłanie powiadomienia w przypadku, gdy skanowanie programem **Arcabit** nic nie wykryło
- 0703 – wysłanie powiadomienia w przypadku połączenia zablokowanego przez zapórę programu **Arcabit**
- 0801 – wysłanie powiadomienia w przypadku zakończenia tworzenia kopii zapasowej w programie **Arcabit**
- 1100 – wysłanie powiadomienia w przypadku błędu aktualizacji repozytorium programu **Arcabit Administrator**
- 1101 – wysłanie powiadomienia w przypadku poprawnej aktualizacji repozytorium programu **Arcabit Administrator**
- 1200 – wysłanie powiadomienia w przypadku błędu aktualizacji programu **Arcabit Administrator**
- 1201 – wysłanie powiadomienia w przypadku poprawnej aktualizacji programu **Arcabit Administrator**
- 1401 – wysłanie powiadomienia w przypadku dopuszczenia urządzenia USB przez program **Arcabit**
- 1403 – wysłanie powiadomienia w przypadku zablokowania urządzenia USB przez program **Arcabit**

- 1501 – wysłanie powiadomienia w przypadku dopuszczenia dostępu do urządzenia multimedialnego przez program **Arcabit**
- 1503 – wysłanie powiadomienia w przypadku zablokowania dostępu do urządzenia multimedialnego przez program **Arcabit**
- 1601 – wysłanie powiadomienia w przypadku dopuszczenia aplikacji przez program **Arcabit**
- 1603 – wysłanie powiadomienia w przypadku zablokowania aplikacji przez program **Arcabit**
- 1701 – wysłanie powiadomienia w przypadku zakończenia czyszczenia systemu przez program **Arcabit**
- 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”