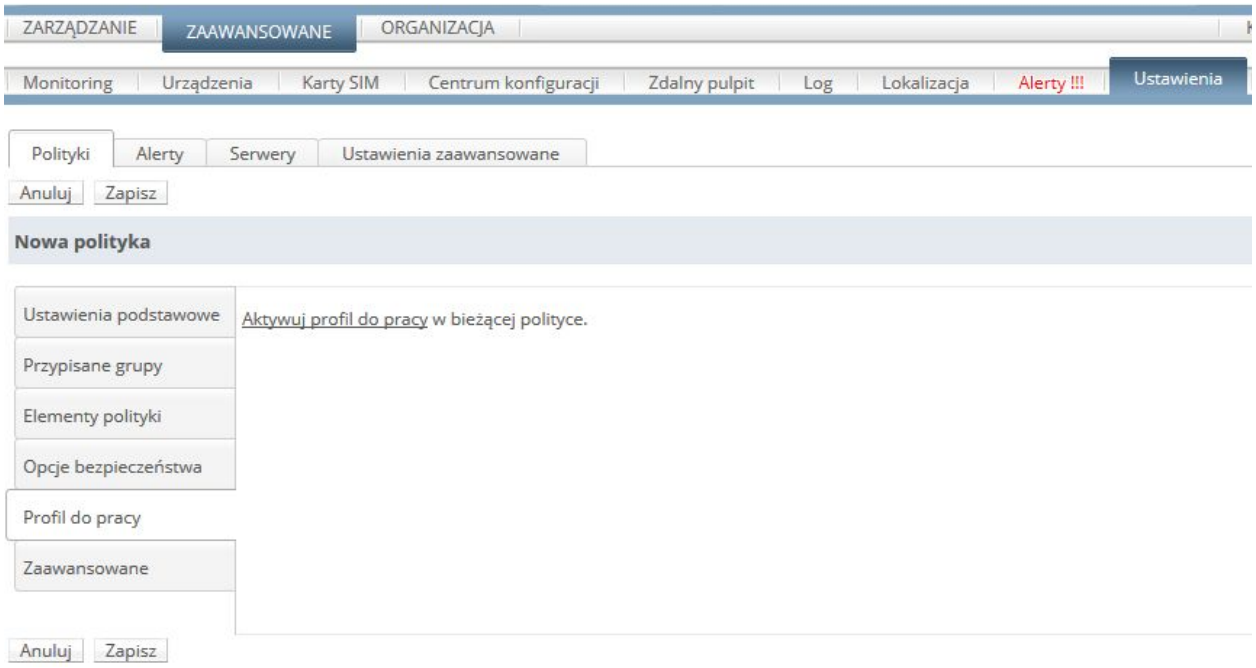
W modelu BYOD pracownicy mogą wykorzystywać do celów zawodowych własne urządzenia mobilne. Aby oddzielić dane prywatne od firmowych zaleca się korzystanie z Profilu do Pracy, narzędzia przeznaczonego do zarządzania przestrzenią służbową na urządzeniach Android. Dzięki systemowi FAMOC z łatwością skonfigurujesz ustawienia Profilu do Pracy zgodnie z Twoimi wymaganiami.

Zanim rozpoczniesz konfigurację polityki Profilu Praca należy powiązać swoje konto FAMOC z Google Enterprise. Jak to zrobić opisano w *Przewodniku Android Enterprise / Profil Praca*. Po zakończeniu tego procesu możliwe jest aktywowanie profilu służbowego w zakładce **Ustawienia** > **Polityki** > **Profil do Pracy**.



Należy pamiętać, że wszelkie ustawienia zostaną zastosowane jedynie do części urządzenia zawartej w Profilu do Pracy.

Ograniczenia profilu służbowego

Aby jak najlepiej zabezpieczyć dane firmowe, zaleca się zablokowanie transferu danych pomiędzy częścią prywatną i służbową. Sugerujemy poniższe ustawienia:

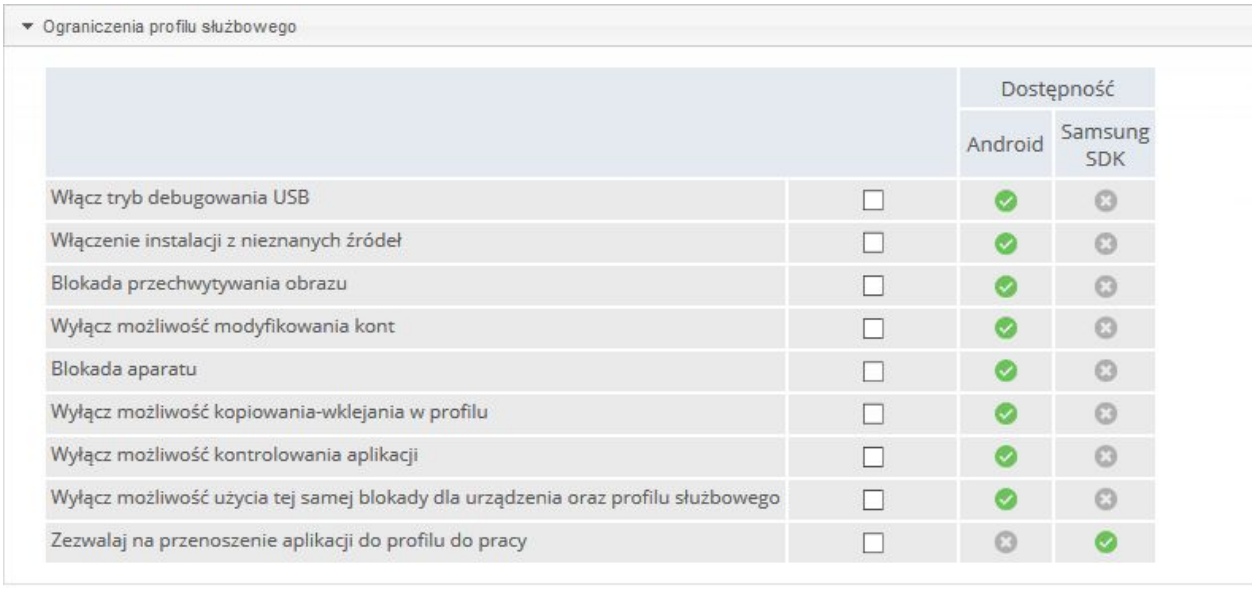
Blokada przechwytywania obrazu - uniemożliwia udostępnienie danych w ten sposób.

Wyłącz możliwość modyfikowania kont - w profilu służbowym funkcjonować będzie jedynie konto firmowe i nie będzie możliwości dokonania zmian.

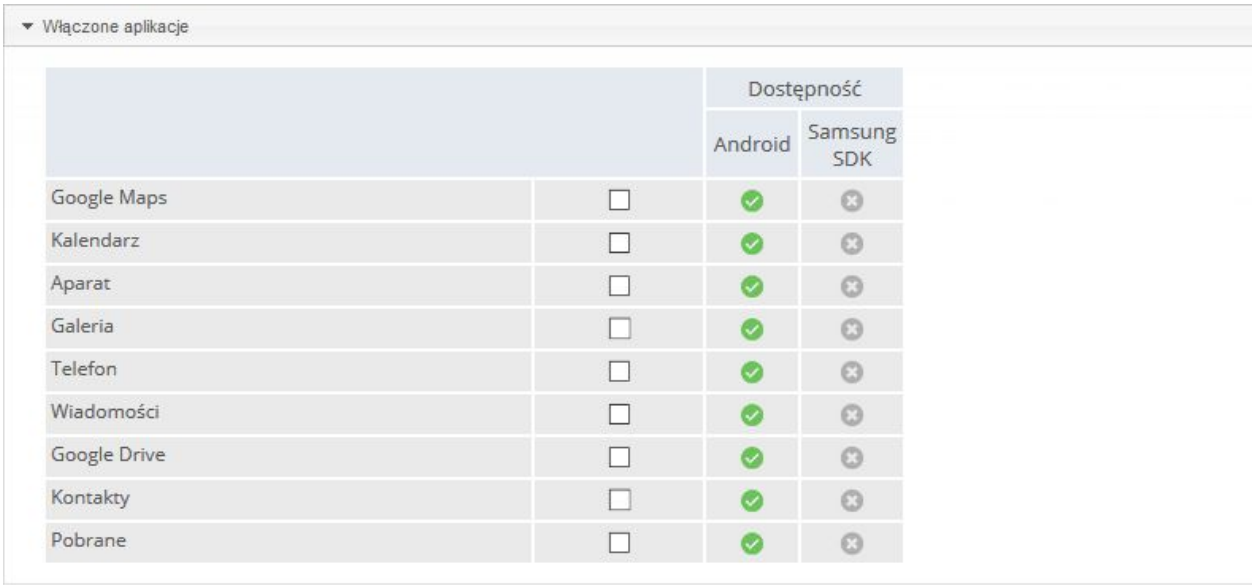
Wyłącz możliwość kopiowania-wklejania w profilu - użytkownik nie będzie mógł przenosić zawartości pomiędzy profilami używając metody kopiuj-wklej.

Wyłącz możliwość kontrolowania aplikacji - użytkownik nie będzie mógł usuwać, wyłączać lub zmieniać ustawień aplikacji.

Globalny dostęp aplikacji: zablokuj - użytkownik nie będzie mógł decydować o uprawnieniach aplikacji.



W zakładce **Włączone aplikacje** znajduje się lista aplikacji systemowych Androida. Domyślnie są one wyłączone i użytkownicy nie mogą korzystać z nich w Profilu Praca. Możesz zdecydować, do których z nich przyznać użytkownikom dostęp.

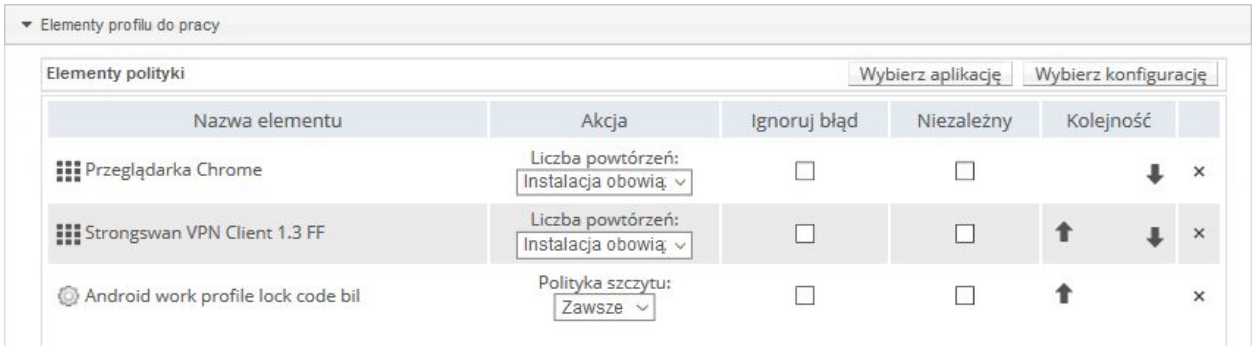


Elementy profilu do pracy

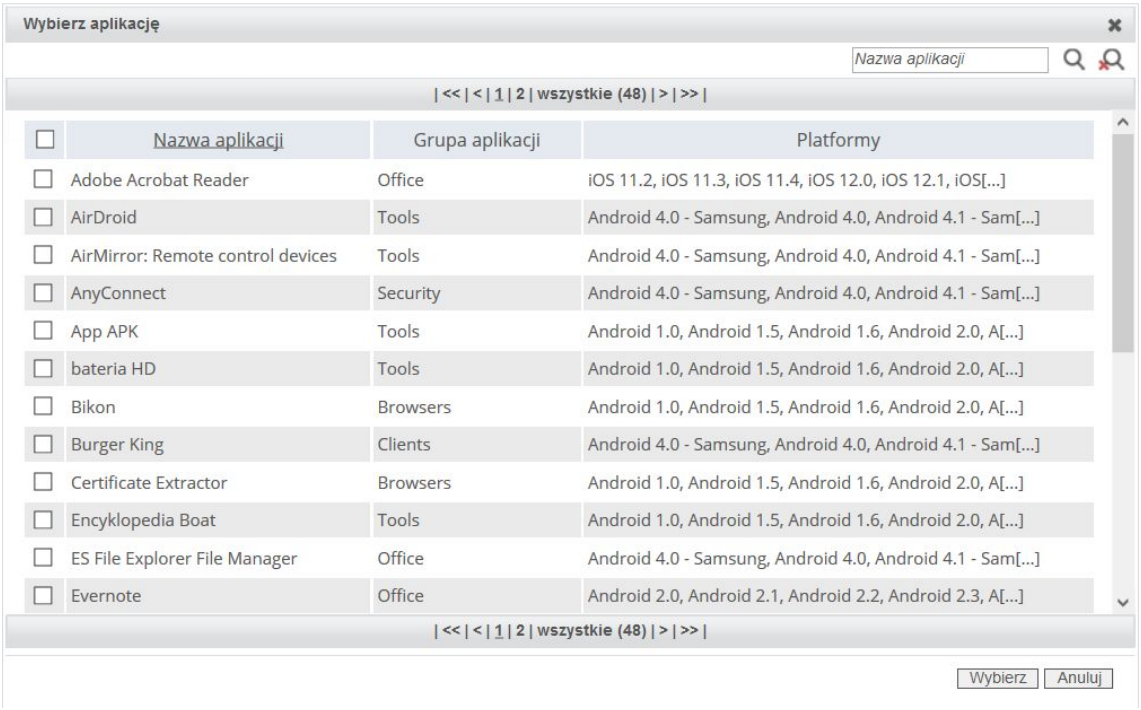
W kolejnej zakładce można skonfigurować **Elementy polityki**. Dostępne elementy to **Aplikacje** oraz **Konfiguracje**.

UWAGA: Możesz wybrać jedynie te aplikacje, które zostały wcześniej dodane do FAMOC-a. Proces dodawania aplikacji został opisany tutaj.

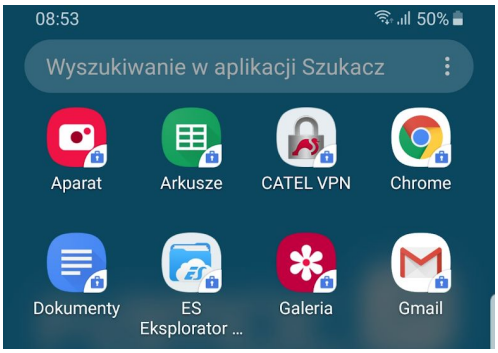
Możesz zdecydować, które aplikacje zostaną zainstalowane na urządzeniu wraz z polityką klikając **Wybierz aplikację**.



Wybierz aplikacje, klikając pole wyboru znajdujące się przy jej nazwie. Aby potwierdzić swój wybór kliknij przycisk **Wybierz**, znajdujący się w prawym dolnym rogu okienka.

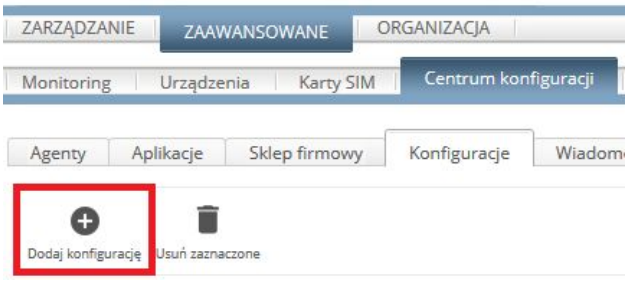


Wybrane aplikacje zostaną zainstalowane w kontenerze Profilu służbowego w momencie zastosowania polityki na urządzeniu i zostaną oznaczone ikoną aktówki.

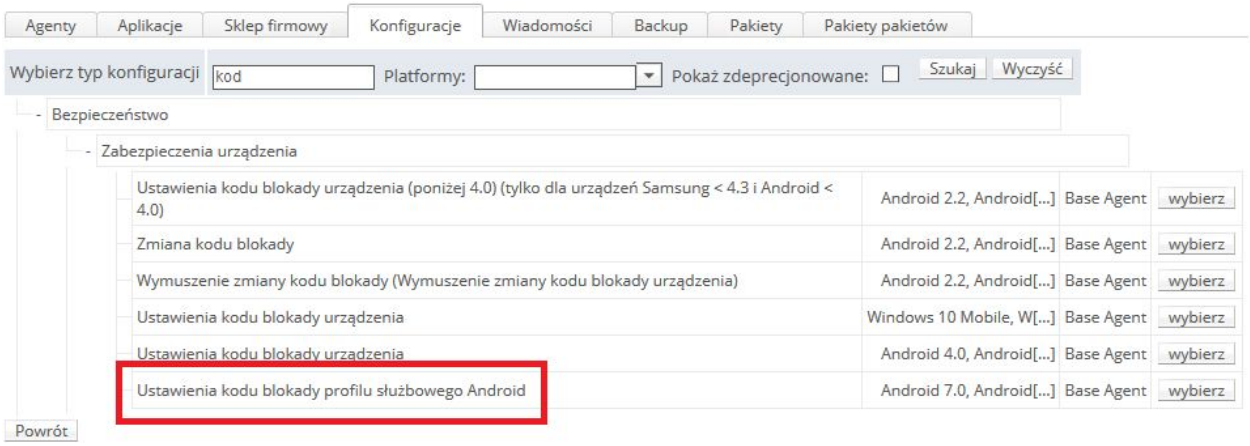


Ustawienia kodu blokady profilu służbowego

Aby zabezpieczyć dostęp do Profilu Praca należy wymusić korzystanie na urządzeniu z **kodu blokady profilu służbowego Android**. Aby skonfigurować ten kod przejdź do zakładki **ZAAWANSOWANE** > **Centrum konfiguracji** > **Konfiguracje**. Kliknij **Dodaj konfigurację**.

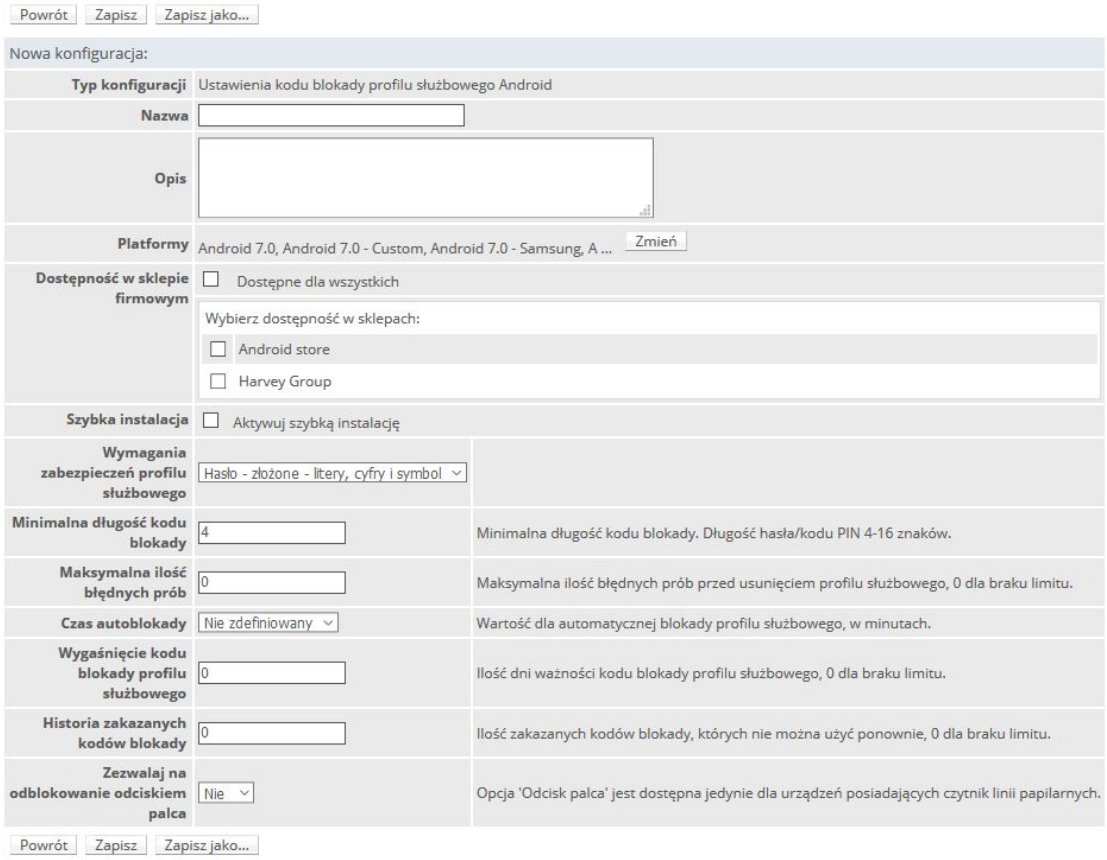


Z menu po lewej stronie wybierz sekcję **Bezpieczeństwo** > **Zabezpieczenia urządzenia**, a następnie wybierz **Ustawienia kodu blokady profilu służbowego Android**.

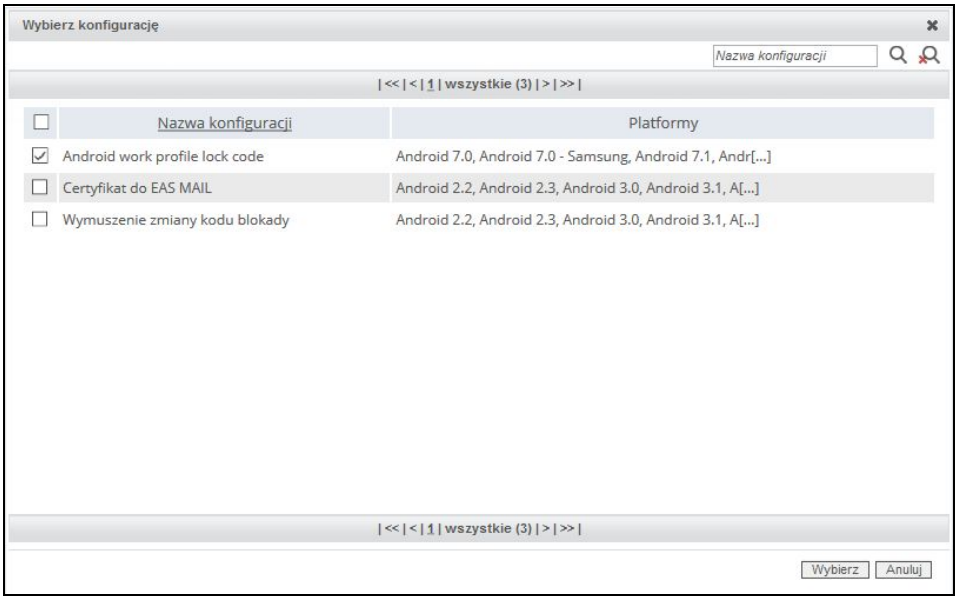


W kolejnym okienku skonfiguruj wymagania kodu blokady. W rozwijanym menu **Wymagania zabezpieczeń profilu służbowego** określ stopień złożoności kodu (litery, litery i cyfry, litery, cyfry i symbole, PIN). Możesz również określić **Minimalna długość kodu blokady** (min.:4 - max.:16 znaków) W przypadku pozostałych opcji można pozostawić wartości domyślne.

Po dokonaniu wyboru kliknij **Zapisz** lub **Zapisz jako…** aby zakończyć konfigurację.



Gdy konfiguracja jest gotowa, należy ją dodać do polityki w taki sam sposób jak aplikacje. W zakładce **Elementy polityki** kliknij **Wybierz konfigurację** zamiast **Wybierz aplikację**. Zaznacz pole wyboru obok konfiguracji, którą chcesz dodać, i potwierdź swój wybór, klikając **Wybierz**.



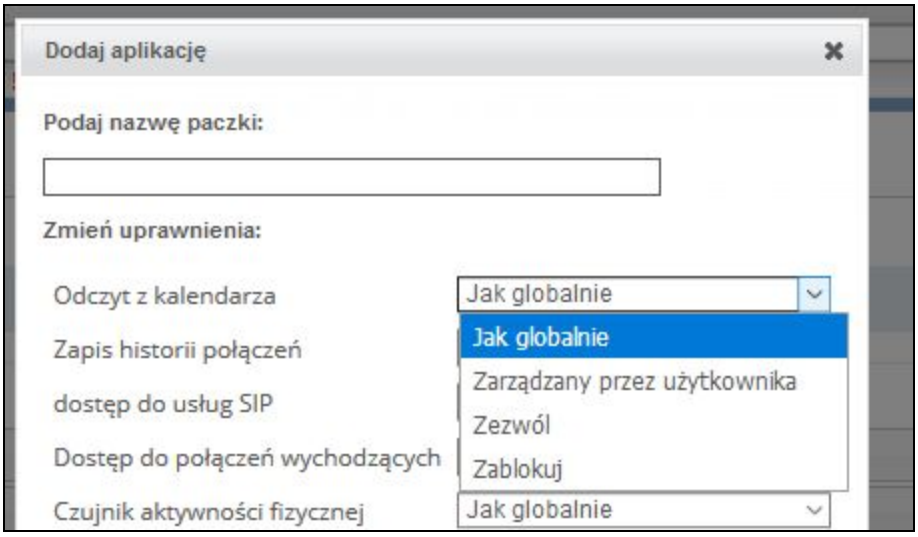
.

Uprawnienia aplikacji

Kolejnym krokiem konfigurowania polityki BYOD jest zarządzanie uprawnieniami aplikacji. Na tej karcie możesz ustawić ograniczenia dla określonej aplikacji, aby zezwolić lub odmówić jej dostępu do niektórych funkcji systemu Android, takich jak Kontakty, Nagrywanie głosu, Kamera itp.

Możesz ustawić **Globalny dostęp aplikacji**:

Możesz także ustawić uprawnienia dla określonych aplikacji. Kliknij Dodaj aplikację. Znajdź aplikację, której szukasz w polu nazwy paczkii skonfiguruj uprawnienia zgodnie z własnymi potrzebami.



Dostępne ustawienia to:

Jako globalnie - uprawnienia są przyznawane zgodnie z globalną polityką uprawnień

Zarządzany przez użytkownika - pozostawia decyzję użytkownikowi

Zezwól - automatyczne zezwolenie

Zablokuj - automatycznie odmawia zgody

W modelu BYOD sugeruje się, aby dać użytkownikom większą swobodę zarządzania swoimi urządzeniami. Jeśli jednak chcesz ograniczyć uprawnienia niektórych aplikacji np. blokując dostęp do kontaktów, kalendarza, danych o lokalizacji itp., możesz to zrobić tutaj.

Gdy wszystko jest skonfigurowane zgodnie z Twoimi potrzebami, nadszedł czas na zapisanie i wdrożenie zasad na urządzeniach. Dzięki zainstalowanemu profilowi pracy części prywatne i firmowe na urządzeniu zostaną rozdzielone, a poufne dane powinny być bezpieczne.