

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**.

The screenshot shows the FAMOC configuration interface. At the top, there are navigation tabs: ZARZĄDZANIE, ZAAWANSOWANE (selected), and ORGANIZACJA. Below these are sub-tabs: Monitoring, Urządzenia, Karty SIM, Centrum konfiguracji, Zdalny pulpit, Log, Lokalizacja, Alerty !!!, and Ustawienia. Under the 'Ustawienia' tab, there are sub-sections: Polityki (selected), Alerty, Serwery, and Ustawienia zaawansowane. There are 'Anuluj' and 'Zapisz' buttons. The main content area is titled 'Nowa polityka' and contains a list of settings: 'Ustawienia podstawowe' (with a link to 'Aktywuj profil do pracy w bieżącej polityce.'), 'Przypisane grupy', 'Elementy polityki', 'Opcje bezpieczeństwa', 'Profil do pracy', and 'Zaawansowane'. At the bottom, there are 'Anuluj' and 'Zapisz' buttons.

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 kopiuuj-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.

		Dostępność	
		Android	Samsung SDK
Włącz tryb debugowania USB	<input type="checkbox"/>	✓	✗
Włączenie instalacji z nieznanymi źródłami	<input type="checkbox"/>	✓	✗
Blokada przechwytywania obrazu	<input type="checkbox"/>	✓	✗
Wyłącz możliwość modyfikowania kont	<input type="checkbox"/>	✓	✗
Blokada aparatu	<input type="checkbox"/>	✓	✗
Wyłącz możliwość kopiowania-wklejania w profilu	<input type="checkbox"/>	✓	✗
Wyłącz możliwość kontrolowania aplikacji	<input type="checkbox"/>	✓	✗
Wyłącz możliwość użycia tej samej blokady dla urządzenia oraz profilu służbowego	<input type="checkbox"/>	✓	✗
Zezwalaj na przenoszenie aplikacji do profilu do pracy	<input type="checkbox"/>	✗	✓

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.

		Dostępność	
		Android	Samsung SDK
Google Maps	<input type="checkbox"/>	✓	✗
Kalendarz	<input type="checkbox"/>	✓	✗
Aparat	<input type="checkbox"/>	✓	✗
Galeria	<input type="checkbox"/>	✓	✗
Telefon	<input type="checkbox"/>	✓	✗
Wiadomości	<input type="checkbox"/>	✓	✗
Google Drive	<input type="checkbox"/>	✓	✗
Kontakty	<input type="checkbox"/>	✓	✗
Pobrane	<input type="checkbox"/>	✓	✗

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](#).

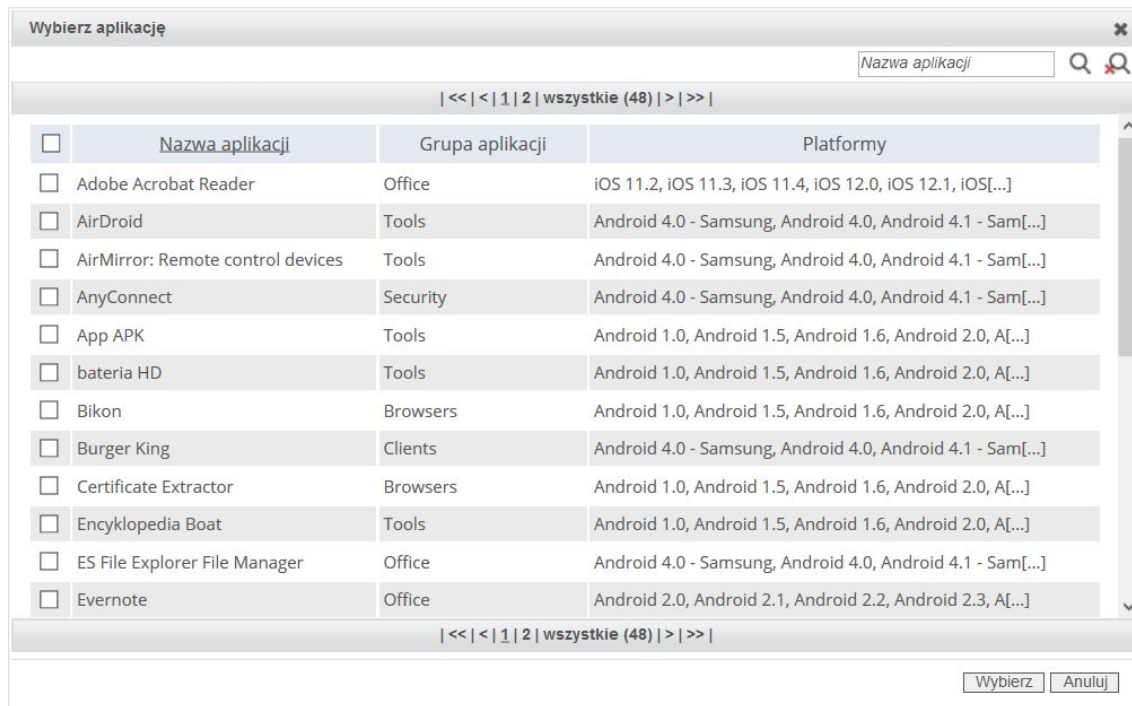
Możesz zdecydować, które aplikacje zostaną zainstalowane na urządzeniu wraz z polityką klikając **Wybierz aplikację**.



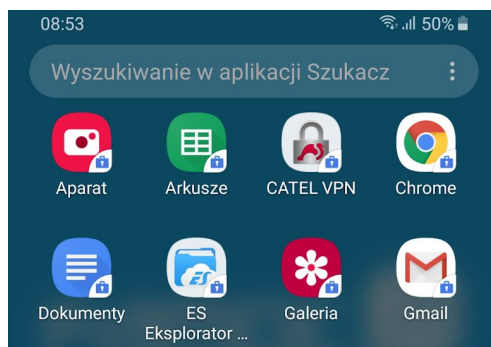
The screenshot shows a window titled 'Elementy profilu do pracy' with a sub-section 'Elementy polityki'. It contains a table with columns: 'Nazwa elementu', 'Akcja', 'Ignoruj błąd', 'Niezależny', 'Kolejność', and an empty column for actions. Three rows are visible:

Nazwa elementu	Akcja	Ignoruj błąd	Niezależny	Kolejność	
Przeglądarka Chrome	Liczba powtórzeń: Instalacja obowią. ▾	<input type="checkbox"/>	<input type="checkbox"/>	↓	×
Strongswan VPN Client 1.3 FF	Liczba powtórzeń: Instalacja obowią. ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑	↓
Android work profile lock code bil	Polityka szczytu: Zawsze ▾	<input type="checkbox"/>	<input type="checkbox"/>	↑	×

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

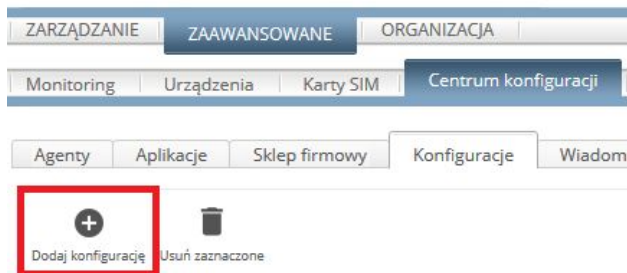


Wybrane aplikacje zostaną zainstalowane w kontenerze Profilu służbowego w momencie zastosowania polityki na urządzeniu i zostaną oznaczone ikoną aktówki.

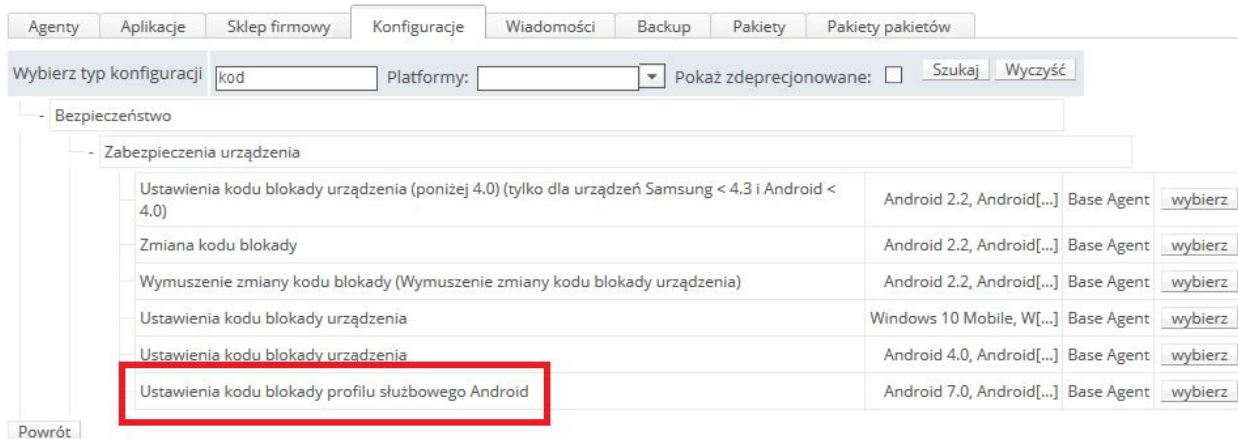


Ustawienia kodu blokady profilu służbowego

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.

Powrót Zapisz Zapisz jako...

Nowa konfiguracja:

Typ konfiguracji	Ustawienia kodu blokady profilu służbowego Android	
Nazwa	<input type="text"/>	
Opis	<input type="text"/>	
Platformy	Android 7.0, Android 7.0 - Custom, Android 7.0 - Samsung, A ... <input type="button" value="Zmień"/>	
Dostępność w sklepie firmowym	<input type="checkbox"/> Dostępne dla wszystkich	
	Wybierz dostępność w sklepach:	
	<input type="checkbox"/> Android store	
	<input type="checkbox"/> Harvey Group	
Szybka instalacja	<input type="checkbox"/> Aktywuj szybką instalację	
Wymagania zabezpieczeń profilu służbowego	<input type="text" value="Hasło - złożone - litery, cyfry i symbol"/>	
Minimalna długość kodu blokady	<input type="text" value="4"/>	Minimalna długość kodu blokady. Długość hasła/kodu PIN 4-16 znaków.
Maksymalna ilość błędnych prób	<input type="text" value="0"/>	Maksymalna ilość błędnych prób przed usunięciem profilu służbowego, 0 dla braku limitu.
Czas autoblokady	<input type="text" value="Nie zdefiniowany"/>	Wartość dla automatycznej blokady profilu służbowego, w minutach.
Wygaśnięcie kodu blokady profilu służbowego	<input type="text" value="0"/>	Ilość dni ważności kodu blokady profilu służbowego, 0 dla braku limitu.
Historia zakazanych kodów blokady	<input type="text" value="0"/>	Ilość zakazanych kodów blokady, których nie można użyć ponownie, 0 dla braku limitu.
Zezwalaj na odblokowanie odciskiem palca	<input type="text" value="Nie"/>	Opcja 'Odcisk palca' jest dostępna jedynie dla urządzeń posiadających czytnik linii papilarnych.

Powrót Zapisz Zapisz jako...

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**.

Wybierz konfigurację

| << | < | 1 | wszystkie (3) | > | >> |

<input type="checkbox"/>	Nazwa konfiguracji	Platformy
<input checked="" type="checkbox"/>	Android work profile lock code	Android 7.0, Android 7.0 - Samsung, Android 7.1, Andr[...]
<input type="checkbox"/>	Certyfikat do EAS MAIL	Android 2.2, Android 2.3, Android 3.0, Android 3.1, A[...]
<input type="checkbox"/>	Wymuszenie zmiany kodu blokady	Android 2.2, Android 2.3, Android 3.0, Android 3.1, A[...]

| << | < | 1 | wszystkie (3) | > | >> |

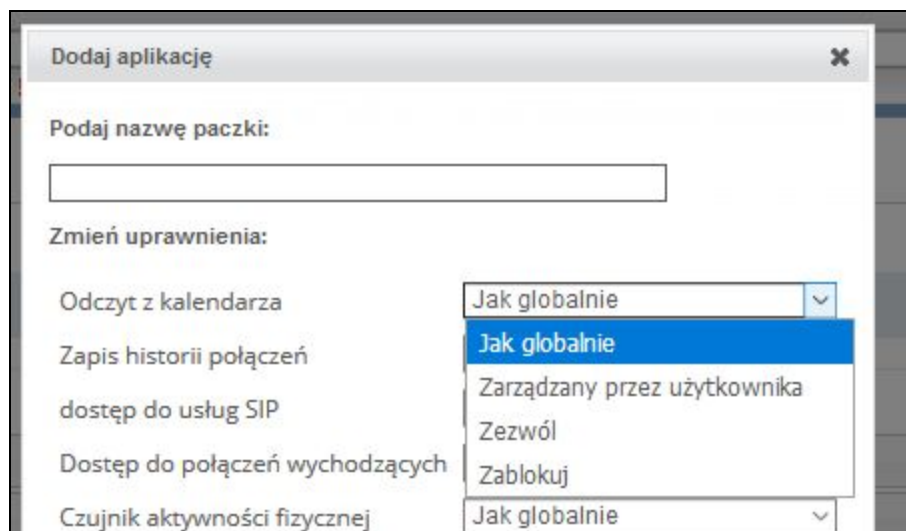
Uprawnienia aplikacji

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 paczki 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.